Red Hat Certificate System 8.1 Using End User Services

for regular users to request and retrieve certificates
Edition 1

Landmann

Red Hat Certificate System 8.1 Using End User Services

for regular users to request and retrieve certificates
Edition 1

Landmann
rlandmann@redhat.com

Legal Notice

Copyright © 2012 Red Hat, Inc..

This document is licensed by Red Hat under the Creative Commons Attribution-ShareAlike 3.0 Unported License. If you distribute this document, or a modified version of it, you must provide attribution to Red Hat, Inc. and provide a link to the original. If the document is modified, all Red Hat trademarks must be removed.

Red Hat, as the licensor of this document, waives the right to enforce, and agrees not to assert, Section 4d of CC-BY-SA to the fullest extent permitted by applicable law.

Red Hat, Red Hat Enterprise Linux, the Shadowman logo, JBoss, MetaMatrix, Fedora, the Infinity Logo, and RHCE are trademarks of Red Hat, Inc., registered in the United States and other countries.

Linux ® is the registered trademark of Linus Torvalds in the United States and other countries.

Java ® is a registered trademark of Oracle and/or its affiliates.

XFS ® is a trademark of Silicon Graphics International Corp. or its subsidiaries in the United States and/or other countries.

MySQL ® is a registered trademark of MySQL AB in the United States, the European Union and other countries.

Node.js ® is an official trademark of Joyent. Red Hat Software Collections is not formally related to or endorsed by the official Joyent Node.js open source or commercial project.

The OpenStack ® Word Mark and OpenStack Logo are either registered trademarks/service marks or trademarks/service marks of the OpenStack Foundation, in the United States and other countries and are used with the OpenStack Foundation's permission. We are not affiliated with, endorsed or sponsored by the OpenStack Foundation, or the OpenStack community.

All other trademarks are the property of their respective owners.

Abstract

This guide contains easy to follow information for end users who use Red Hat Certificate System certificate authority and registration authority services to generate or submit certificate requests, check on request status, receive certificates, and revoke certificates.

Table of Contents

1. A Look at End User Services in Red Hat Certificate System 2
1.1. About Certificates and Cryptography 2
1.2. About CA Services 5
1.3. About RA Services 8
1.4. Supported Web Browsers 8
1.5. Supported Charactersets 9
1.6. Configuring Internet Explorer to Enroll Certificates 9

2. Getting and Managing Certificates through CA Services 10
2.1. Opening the CA Services Page 10
2.2. Generating Certificate Requests 10
2.3. Requesting Certificates 12
2.4. Checking on Your Request Status 14
2.5. Retrieving Your Certificates 15
2.6. Listing and Searching for Certificates 16
2.6.1. Listing Certificates (Basic Search) 16
2.6.2. Searching for Certificates (Advanced Search) 17
2.7. Renewing Certificates 20
2.7.1. Agent-Approved or Directory-Based Renewals 21
2.7.2. Certificate-Based Renewal 22
2.8. Revoking Certificates 23
2.8.1. Revoking Your User Certificate 23
2.8.2. Checking Whether a Certificate Is Revoked 24
2.8.3. Downloading and Importing CRLs 25
2.9. Downloading CA Certificates and Certificate Chains 27

3. Getting and Managing Certificates through RA Services 28
3.1. Opening the RA Services Page 28
3.2. Requesting Certificates 28
3.2.1. Requesting User Certificates 28
3.2.2. Requesting Server Certificates 29
3.2.3. Requesting SCEP (Router) Certificates 30
3.2.4. Requesting Agent Certificates 34
3.3. Checking on Your Request Status 36
3.4. Retrieving and Importing Certificates 37
3.5. Renewing User Certificates 39

4. Additional Reading 41

5. Giving Feedback 42

6. Document History 42

1. A Look at End User Services in Red Hat Certificate System

Red Hat Certificate System provides a simple way for people to obtain certificates that they need to protect common Internet-based actions, like sending email, logging into a computer, or accessing a protected website. Any user can access Certificate System's web-based certificate management interface to request or receive a certificate.

1.1. About Certificates and Cryptography

Red Hat Certificate System provides a way for a company or group to create and manage certificates locally.

A *certificate* is a file which proves the identity of a person, server, router, website, or other entity. Certificates can also be used to encrypt and decrypt information; this is a vital function which protects sensitive communication — from online shopping to email — by safely encoding the traffic using mathematical algorithms to create a cipher.

A certificate is part of an overall strategy for *secure* (encrypted) communication. Some web protocols such as Secure Sockets Layer (SSL) and Transport Layer Security (TLS) use encryption to secure Internet communications, as do VPNs, some intranets, email, and web browsers.

Secure communications are built around an *SSL handshake*. An SSL handshake is when a server reaches out to a client (user) with some proof of its identity, such as a certificate; this is *server authentication*. The client can then accept that certificate to continue with the connection. The server may require some proof back from the user to verify his identity; this is *client authentication*. After the server and client are shown to be authentic, then they can continue with their transactions.

The transactions are encoded using agreed upon methods, called *ciphers*. The cipher is used in conjunction with a special number, called a key, to encrypt and decrypt the data being sent. A certificate, along with identifying the user and the authority which issued it, defines what kind of ciphers it supports and the public key for encrypting information.

There are a number of different ways that the information can be encrypted for safe sending and then decrypted for safe reading: asymmetric keys, symmetric keys, and shared keys. A key, in broad terms, is combined with a mathematical algorithm to scramble data; if someone knows the matching key, then they can use it to unscramble the data. A key, then, locks and unlocks data. A *public key* is known to both groups in a secure connection, while a *private key* is held by one group. The public key encrypts data; the private key is used to decrypt it.

A certificate is created out of several pieces of information:

- The identity of the entity (such as its name)
- A public key
- The name and digital signature of the certificate authority which issued the certificate
- The day that the certificate expires (called the *validity period*)
- A serial number

This information creates a *fingerprint* for the certificate.

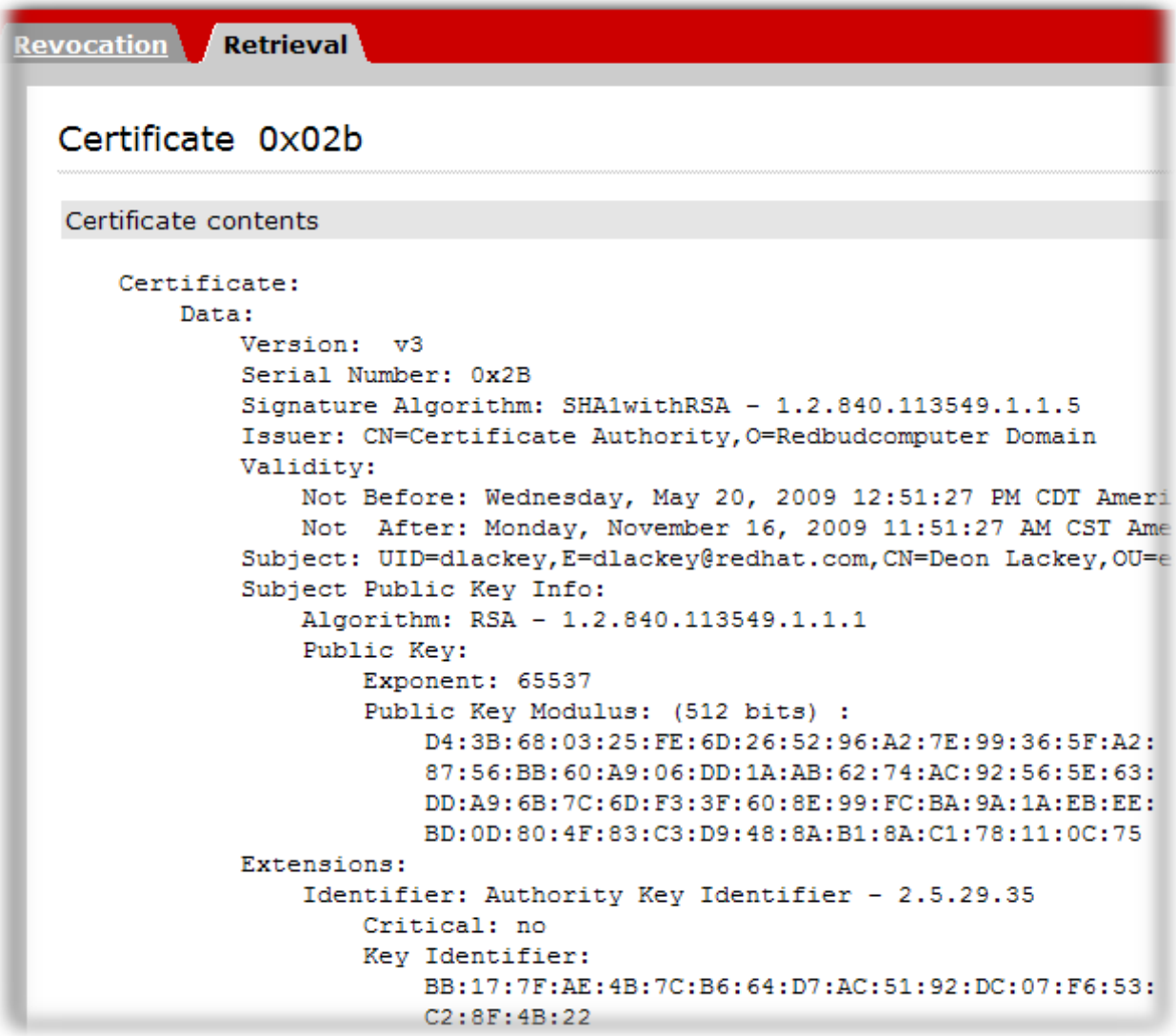


Figure 1. Certificate Fingerprint

Some clients may require additional information, such as the issuing authority's certificate (CA certificate). The CA certificate verifies the server which issued the user's certificate and provides some key information. Sometimes, a series of authorities issues certificates; Server 1 issues a certificate to Server 2 which issues a certificate to Server 3. All of those successive CA certificates can be downloaded and installed together; that's a *certificate chain*.

A certificate is issued or *enrolled* by a certificate authority (CA). (In Red Hat Certificate System, the CA is performed by a system called the Certificate Manager.)

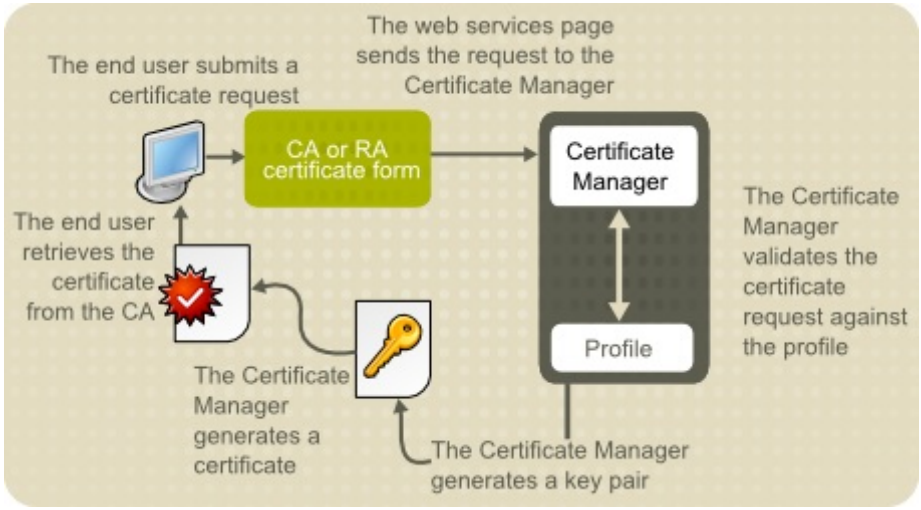

The end user submits a certificate request
The web services page sends the request to the Certificate Manager
CA or RA certificate form
Certificate Manager
The Certificate Manager validates the certificate request against the profile
Profile
The end user retrieves the certificate from the CA
The Certificate Manager generates a certificate
The Certificate Manager generates a key pair

Figure 2. The Process for Issuing a Certificate

1. A user first generates a certificate request by supplying certain information.
2. This request is then given to the CA, and the CA validates that it is a legitimate request. This can happen in different ways: a real person may review it, it could be guaranteed automatically, or it could require that the user supply some other kind of credentials, such as login information for a local directory or an existing certificate.
3. Assuming that the request is approved, the certificate is generated. A Certificate System Certificate Manager uses *certificate profiles* to define the settings for a certificate. The profiles, to users, are simple forms available through the CA services pages. In the Certificate Manager server, these profiles define all kinds of information about the certificate, such as how long the certificate is valid, what kind of ciphers it allows, what kind of certificate it is and how it can be used, and limits set on the certificate information.

   The information in the certificate request must match the requirements in the certificate profile; otherwise, the certificate is rejected by the Certificate Manager.
4. If the certificate request conforms to the profile, then the Certificate Manager signals the browser to generate the public/private key pair.
5. After generating the keys, the Certificate Manager generates the certificate.
6. The user retrieves the new certificate. This varies depending on how the local Red Hat Certificate System is setup; the user may receive an email notification or the certificate could be immediately available through the Certificate Manager services page. The certificate can always be retrieved by searching the request ID and following the status link.
7. The certificate can be imported into a web browser, email program, site, server, router, or other client (depending on the type of certificate) and it's ready for use.

After the certificate is created, it is valid for a certain amount of time, until the expiration date. Some types of certificates can be *renewed*, which creates a new certificate using the same key pair, but with a new expiration date and serial nu,ber. The renewed certificate is functionally identical to the original certificate.

Alternatively, there can be a reason to invalidate a certificate before its expiration date, maybe because it was compromised or because of a change in the user's situation. In that case, the certificate can be revoked before its expiration date. When a certificate is revoked, the Certificate Manager adds it to a list of revoked certificates called a *certificate revocation list* (CRL). When a certificate is validated during authentication, the server checks its validity date (to make sure its current) and its revocation status (by checking the CRL published by the CA).

1.2. About CA Services

A certificate authority (CA) is a trusted entity that issues certificates, verifies the certificate validity, renews certificates, and publishes certificate revocation lists (CRLs). The CA performs all certificate management functions. In Red Hat Certificate System, the CA is called the Certificate Manager.

The Certificate Manager's web services pages offer a number of different services for users:

- Submit requests for a large number of different certificate types through different *certificate enrollment forms* (listed in Table 1, “Available Certificate Profiles”)
- Check the status of certificate requests
- List all submitted certificate requests
- Perform basic and advanced searches of certificate requests, issued certificates, CRLs, and expired certificates
- Retrieve and import issued certificates
- Search CRLs for revoked certificates
- Download, import, or view CRLs
- Download, import, or view CA certificates and CA certificate chains

The Certificate Manager's end user web services offer a large number of default certificate submission forms (called *certificate enrollment forms* or *certificate profiles*). These forms allow you to submit new certificate requests to the CA. Along with the default profiles in Table 1, “Available Certificate Profiles”, custom profiles can also be created that are specific for your group.

The Certificate Manager web services have a very flexible search feature to list and search all certificate requests. The CA web services also allow you to import CA certificates and CA chains, revoke certificates and check certificate revocation status, and import CRLs.

Table 1. Available Certificate Profiles

Profile Name	Description
Security Domain Administrator Certificate Enrollment	Enrolls Security Domain Administrator's certificates with LDAP authentication against the internal LDAP database.
Agent-Authenticated File Signing	This certificate profile is for file signing with agent authentication.
Agent-Authenticated Server Certificate Enrollment	Enrolls server certificates with agent authentication.
Manual Certificate Manager Signing Certificate Enrollment	Enrolls Certificate Authority certificates.
Signed CMC-Authenticated User Certificate Enrollment	Enrolls user certificates by using the CMC certificate request with CMC Signature authentication.
Directory-Authenticated User Dual-Use Certificate Enrollment	Enrolls user certificates with directory-based authentication.
Directory-Authenticated User Certificate Self-Renew profile	Renews user certificates which were previously enrolled with the caDirUserCert profile.
Manual User Signing & Encryption Certificates Enrollment	Enrolls dual user certificates. It works only with Netscape 7.0 or later.
Signed CMC-Authenticated User Certificate Enrollment	Enrolls user certificates by using the CMC certificate request with CMC Signature authentication.
Manual Security Domain Certificate Authority Signing Certificate Enrollment	Enrolls Security Domain Certificate Authority certificates.
Audit Signing Certificate Enrollment	Enrolls a signing certificate to use for signing audit logs; used automatically during any subsystem configuration, with the exception of the RA.
Security Domain DRM Storage Certificate Enrollment	Enrolls DRM storage certificates for DRMs within a security domain; used automatically during a DRM configuration.
Security Domain OCSP Manager Signing Certificate Enrollment	Enrolls Security Domain OCSP Manager certificates.
Security Domain Server Certificate Enrollment	Enrolls Security Domain server certificates.
Security Domain Subsystem Certificate Enrollment	Enrolls Security Domain subsystem certificates.
Security Domain Data Recovery Manager Transport Certificate Enrollment	Enrolls Security Domain Data Recovery Manager transport certificates.
Renew certificate to be manually approved by agents	Renews a certificate that was generated with the caUserCert profile and must be manually renewed by agents.
Manual OCSP Manager Signing Certificate Enrollment	Enrolls OCSP Manager certificates.
Other Certificate Enrollment	Enrolls other certificates.
Manual Registration Manager Signing Certificate Enrollment	Enrolls Registration Manager certificates.
One Time Pin Router Certificate Enrollment	Enrolls router certificates using an automatically-generated, one-time PIN that the router can use

	to retrieve its certificate.
Manual Server Certificate Enrollment	Enrolls server certificates.
Manual Log Signing Certificate Enrollment	Enrolls audit log signing certificates.
Simple CMC Enrollment	Enrolls user certificates by using the CMC certificate request with CMC Signature authentication.
Self-renew user SSL client certificates	Renews SSL client certificates issued by the caUserCert profile.
Temporary Device Certificate Enrollment	Enrolls temporary keys to be used by servers or other network devices on a token; used by the TPS for smart card enrollment operations. These are temporary keys, valid for about a week, and intended to replace a temporarily lost token.
Enrolls an encryption key on a token; used by the TPS for smart card enrollment operations. These are temporary keys, valid for about a week, and intended to replace a temporarily lost token.	
Temporary Token User Signing Certificate Enrollment	Enrolls a signing key on a token; used by the TPS for smart card enrollment operations. These are temporary keys, valid for about a week, and intended to replace a temporarily lost token.
Token Device Key Enrollment	Enrolls keys to be used by servers or other network devices on a token; used by the TPS for smart card enrollment operations.
Token User MS Login Certificate Enrollment	Enrolls key to be used by a person for logging into a Windows domain or PC; used by the TPS for smart card enrollment operations.
Token User Encryption Certificate Enrollment	Enrolls an encryption key on a token; used by the TPS for smart card enrollment operations.
smart card token encryption cert renewal profile	Renews an encryption key that was enrolled on a token using the caTokenUserEncryptionKeyEnrollment profile; used by a TPS subsystem.
Token User Signing Certificate Enrollment	Enrolls a signing key on a token; used by the TPS for smart card enrollment operations.
smart card token signing cert renewal profile	Renews a signing that was enrolled on a token using the caTokenUserSigningKeyEnrollment profile; used by a TPS subsystem.
Manual TPS Server Certificate Enrollment	Enrolls TPS server certificates.
Manual Data Recovery Manager Transport Certificate Enrollment	Enrolls Data Recovery Manager transport certificates.
Manual User Dual-Use Certificate Enrollment	Enrolls user certificates.
Manual device Dual-Use Certificate Enrollment to contain UUID in SAN	Enrolls certificates for devices which must contain a unique user ID number (UUID) as a component in the certificate's subject alternate name extension.
Domain Controller	Enrolls certificates to be used by a Windows domain controller.

1.3. About RA Services

The Red Hat Certificate System Registration Authority (RA), similar to the Certificate Manager, can accept certificate requests. The RA doesn't issue or enroll the certificates; instead, it authenticates the entity making the request locally, then forwards the request to the CA to generate the certificate. The RA is in essence a load balancer for certificate management.

The RA web services page offers several different options:

- Submit certificate requests and renew certificates (through enrollment forms listed in Table 2, “Available RA Certificate Profiles”)
- Check the status of pending certificate requests
- Retrieve issued certificates

The RA has fewer certificate enrollment options than the Certificate Manager, and the RA interface is more simple than the Certificate Manager's web services pages. The benefit of the RA interface is that it can be quicker to submit requests, receive approval, check request status, and retrieve issued certificates.

The RA is essentially a load balancer for a CA, since the CA still issues the certificates but the process of approving the certificate request is handled separately.

Table 2. Available RA Certificate Profiles

Profile Name	Description
User Enrollment	Enrolls and renews user certificates.
Server Certificate Enrollment	Enrolls server certificates.
RA Agent Enrollment	Enrolls certificates for RA agents.
SCEP Enrollment	Enrolls router certificates, complying with Cisco SCEP standards.

1.4. Supported Web Browsers

The services pages for the subsystems require a web browser that supports SSL. Two browsers are supported:

- Mozilla Firefox 1.0 and higher
- Microsoft Internet Explorer 6 and higher

NOTE

Browsers for Mac, such as Safari, and other types of web browsers, such as Opera, are not supported for the end-entities pages. This means that some operations may not complete successfully or forms may not be displayed properly.

If DNS is properly configured, then an IPv4 or IPv6 address can be used to connect to the services pages. For example:

```
https://1.2.3.4:9444/ca/services
https://[00:00:00:00:123:456:789:00:]:9444/ca/services
```

1.5. Supported Charactersets

Red Hat Certificate System fully supports UTF-8 characters in the CA end users forms for specific fields. This means that end users can submit certificate requests with UTF-8 characters in those fields and can search for and retrieve certificates and CRLs in the CA and retrieve keys in the DRM when using those field values as the search parameters.

Four fields fully-support UTF-8 characters:

- Common name (used in the subject name of the certificate)
- Organizational unit (used in the subject name of the certificate)
- Requester name
- Additional notes (comments appended by the agent to the certificate)

NOTE

This support does not include supporting internationalized domain names, like in email addresses.

1.6. Configuring Internet Explorer to Enroll Certificates

Because of the security settings in Microsoft Windows Vista, requesting and enrolling certificates through the end entities pages using Internet Explorer 7 and 8 requires extra browser configuration. The browser has to be configured to trust the CA before it can access the CA's secure end entities pages.

NOTE

This configuration is not necessary to use Internet Explorer 7 and 8 on Microsoft Windows 2000, 2003, or XP.

1. Open Internet Explorer.
2. Import the CA certificate chain.
    a. Open the unsecure end services page for the CA.

    ```
    http://server.example.com:9180/ca/ee/ca
    ```

    b. Click the **Retrieval** tab.
    c. Click **Import CA Certificate Chain** in the left menu, and then select **Download the CA certificate chain in binary form**.
    d. When prompted, save the CA certificate chain file.
    e. In the Internet Explorer menu, click **Tools**, and select **Internet Options**.
    f. Open the **Content** tab, and click the **Certificates** button.
    g. Click the **Import** button. In the import window, browse for and select the imported certificate chain.

    The import process prompts for which certificate store to use for the CA certificate chain. Select **Automatically select the certificate store based on the type of certificate**.
    h. Once the certificate chain is imported, open the **Trusted Root Certificate**

Authorities tab to verify that the certificate chain was successfully imported.

3. After the certificate chain is imported, Internet Explorer can access the secure end services pages. Open the secure site.

```
https://server.example.com:9443/ca/ee/ca
```

4. There is probably a security exception when opening the end services pages. Add the CA services site to Internet Explorer's **Trusted Sites** list.
    a. In the Internet Explorer menu, click **Tools**, and select **Internet Options**.
    b. Open the **Security** tab, and click **Sites** to add the CA site to the trusted list.
    c. Set the **Security level for this zone** slider for the CA services page to **Medium**; if this security setting is too restrictive in the future, then try resetting it to **Medium-low**.
5. Close the browser.

To verify that Internet Explorer can be used for enrollments, try enrolling a user certificate, as described in Section 2.3, “Requesting Certificates”.

2. Getting and Managing Certificates through CA Services

The Certificate Manager is the subsystem which functions as a certificate authority in Red Hat Certificate System and issues and manages certificates.

2.1. Opening the CA Services Page

The URL for the CA web services can vary depending on your group's server deployment. The default way to connect to the CA web services is to connect to the server over port 9180. For example:

```
https://server.example.com:9180/
```

That opens a menu with links to regular user services or agent services. To get directly to the regular user pages, add **/ca/ee/ca/** to the end of the URL. For example:

```
https://server.example.com:9180/ca/ee/ca/
```

If DNS is properly configured, then an IPv4 or IPv6 address can be used to connect to the services pages, as well as a hostname or fully-qualified domain name. For example:

```
https://1.2.3.4:9444/ca/services
https://[00:00:00:00:123:456:789:00:]:9444/ca/services
```

2.2. Generating Certificate Requests

Most user profiles in the CA do not require you to generate a certificate request separately. However, there can be situations where you need to request a certificate that doesn't match the default configuration in the certificate profiles. In that case, you can generate a certificate request and submit it using the Other Certificates profile.

One common example is requesting an ECC certificate. *Elliptic curve cryptography* (ECC) is a strong cryptographic algorithm which is very secure and very fast. By default, a Certificate System CA issues RSA certificates (a different cryptographic algorithm), but a CA can be configured to support ECC as well. The CA profiles, however, will only generate RSA keys for a certificate, even though they can process both RSA and ECC requests. So, if you want an ECC certificate, you need to prepare a separate certificate request (and generate the ECC keys) and then submit it through the certificate profile.

Windows and Red Hat Enterprise Linux both have a tool called **certutil** that can generate certificate requests, with slightly different options and settings. There may also be tools or services in your organization that generate certificate requests.

For example (and this command should all be on one line):

```
certutil -R -k ec -g 256 -s "CN=example cert server.example.com,
e=admin@example.com, O=Example Domain" -o request.cert -v 12 -d . -1 -7 -8
```

For information about using the **certutil** command, see http://www.mozilla.org/projects/security/pki/nss/tools/certutil.html.

Table 3. Options for Requesting Certificates with certutil

Option	Description
-R	Flag to generate a certificate request.
-k	The key type to use; the only native option is **rsa**. If the CA is ECC-enabled (described in the *Installation Guide*), then this can also be **ec**.
-g	The key size. The recommended size for RSA keys is 2048 and for ECC, 256.
-s	The subject name of the certificate. **NOTE** Certificate System supports all UTF-8 characters for the common name and organizational unit elements included in the subject name of the certificate.
-o	The output file to which to save the certificate request.
-v	The validity period, in months.
-d	Certificate database directory; this is the directory for the subsystem instance.
numbers 1-8	These set the available certificate extensions. Only eight can be specified through the **certutil** tool: - Key Usage: 1 - Basic Constraints: 2 - Certificate Authority Key ID: 3 - CRL Distribution Point: 4 - Netscape Certificate Type: 5 - Extended Key Usage: 6 - Email Subject Alternative Name: 7 - DNS Subject Alternative Name: 8
-a	Outputs the certificate request to an ASCII file instead of binary.

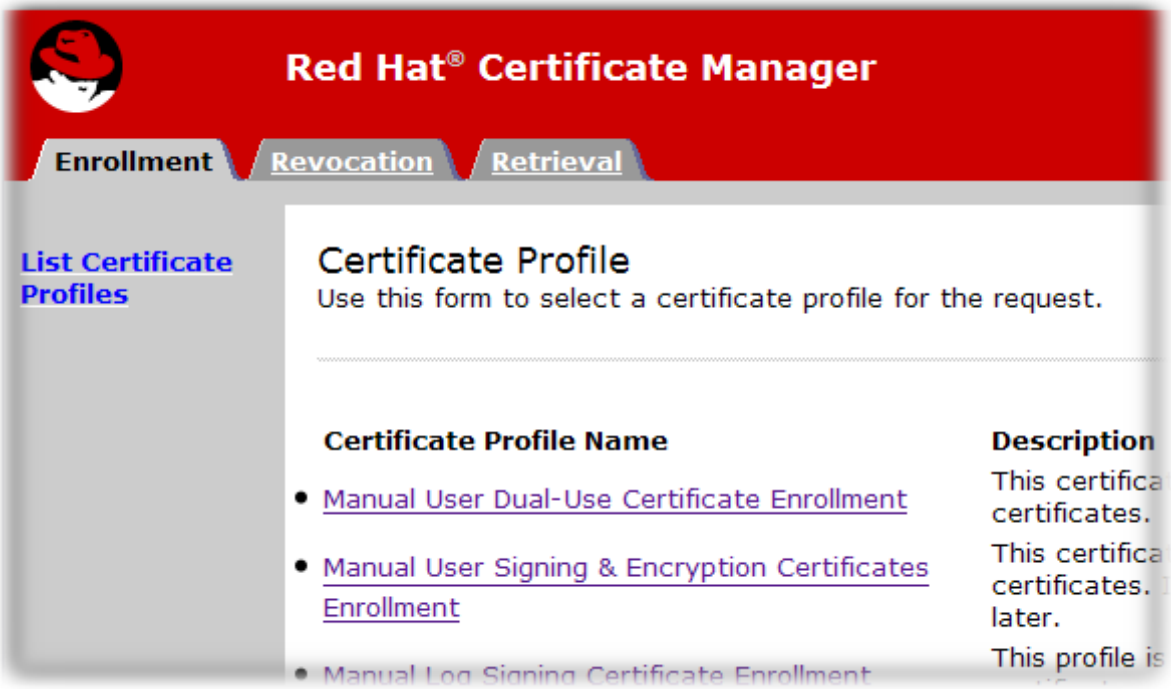
2.3. Requesting Certificates

Certificate requests are submitted to the Certificate Manager through the forms listed in the **`Enrollment`** tab. The Certificate Manager has a variety of different certificate request submission forms (called *certificate profiles*). The type of form to use depends on the type of certificate you need. The different certificate profiles are listed in Table 1, “Available Certificate Profiles”.

Most user certificates can be requested directly through the enrollment forms; there is no need to generate a separate certificate request. Other types of certificates (especially certificates for servers or applications), may require generating a separate certificate request, and then submitting that through the enrollment form. Generating certificate requests is covered in Section 2.2, “Generating Certificate Requests”.

To submit a certificate request:

1. Click the name of the submission form to use.

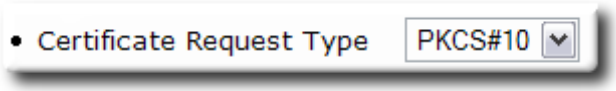


2. Fill in the information required for the certificate.

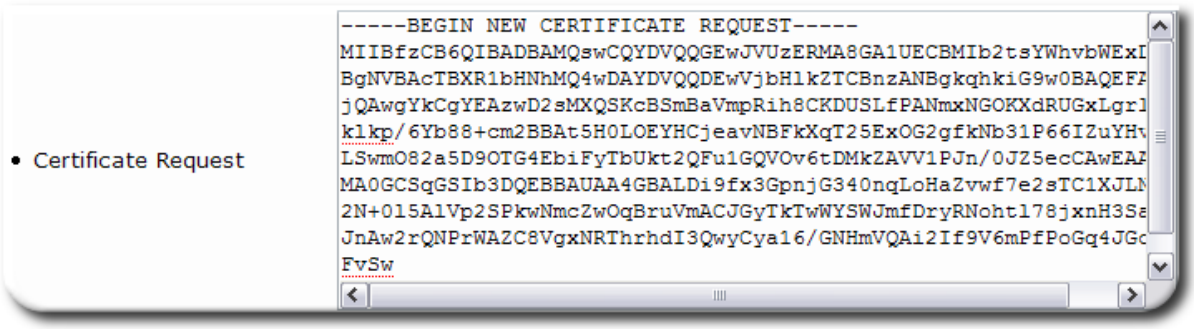
   There are basically two kinds of certificate enrollment forms. One kind accepts certificate request blobs, and the other requires additional user information to build the subject name of the certificate (a major part of its identifier).

   To submit a certificate request:

   - Set the certificate format to generate. There are two options, PKCS #10 (the most common one) or CRMF.



   - Paste in the base 64-encoded certificate request.

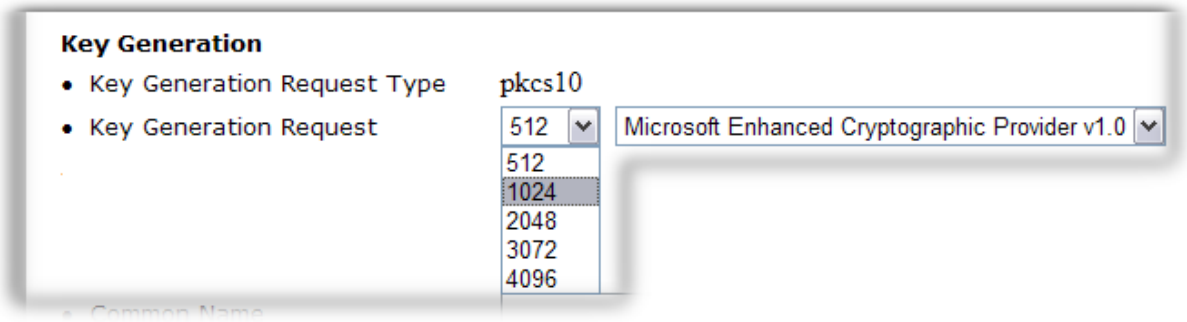


NOTE

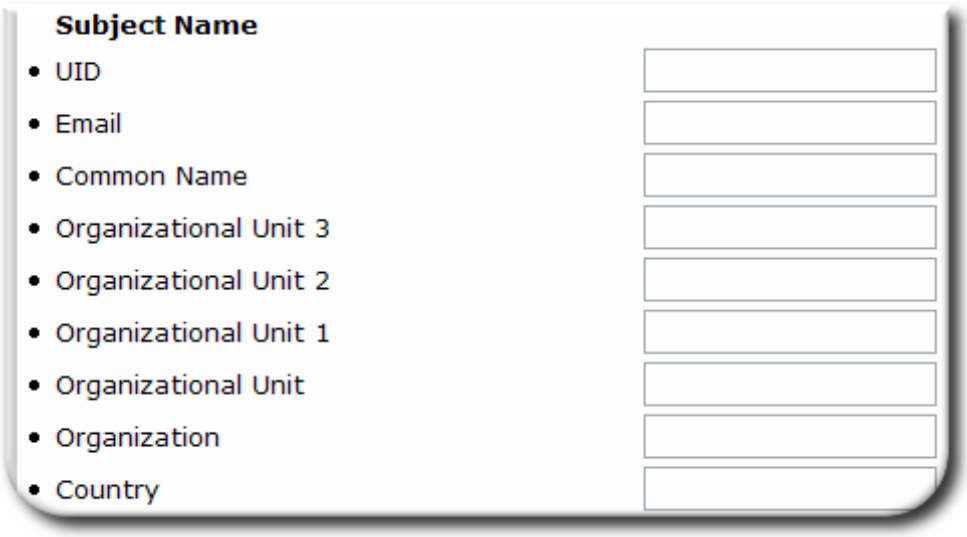
The way that you generate the base 64-encoded certificate request depends on your network setup. There may be an online form you can use to create a certificate request, the client you are requesting the certificate for may have a built-in request tool, or you can use tools such as **`certutil`**. The options for creating a certificate request are covered more in the *Certificate System Administrator's Guide*.

For other types of certificate profiles, the form requires information about the requester in order to create the subject name of the new certificate. [1]

- The certificate format may be automatically set to PKCS#10 or CRMF, depending on the profile, and the key size is selected by the requester.



- Fill in the subject name information, such as the username (UID), email address, location, and organization information.

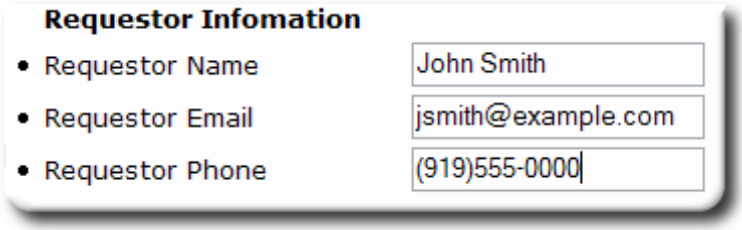


Other forms may require other information. For example, file signing profiles require a URL to the external file that will be signed by the CA.

NOTE

The CA certificate request forms support all UTF-8 characters for the common name, organizational unit, and requester name fields.
This support does not include supporting internationalized domain names.

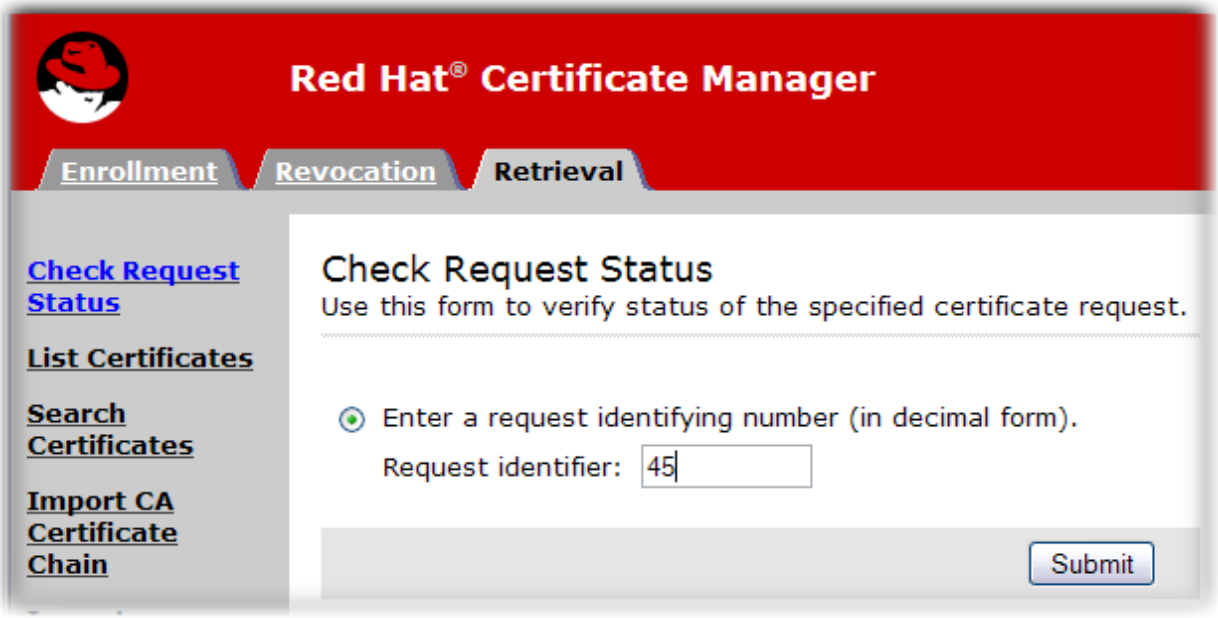
3. For every certificate enrollment, fill in the requester information. All certificate forms take the name, phone number, and email address of the requester. The email address may be required if you will be notified by email when the certificate is issued.



4. Click the **Submit** button.

2.4. Checking on Your Request Status

1. Click the **Retrieval** tab.
2. Enter the request ID number (the one returned when you submitted the request) in the **Request identifier** field. To search for or list requests, see Section 2.6, “Listing and Searching for Certificates”.



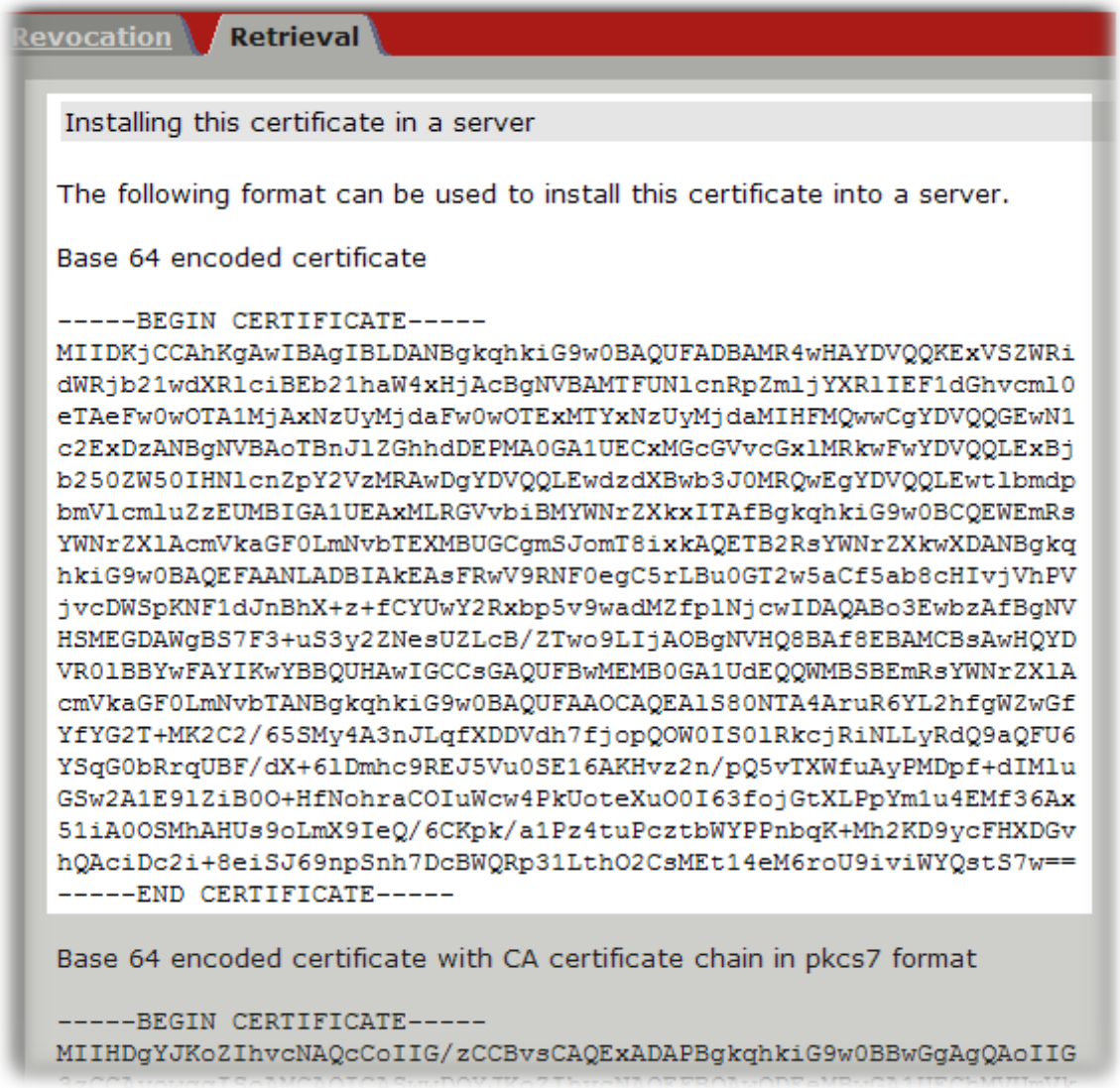
3. The request status is shown as pending, rejected, or completed. If the request has been completed, click the link to retrieve the issued certificate.

2.5. Retrieving Your Certificates

After a certificate is generated by the Certificate Manager, it can be copied to a file or imported directly into your browser.

1. Click the **`Retrieval`** tab in the CA web services page.
2. Open the certificate, either by checking the status and opening it or by finding it in a list of issued certificates.
3. The certificate page has three major sections: the certificate fingerprint, the base 64-encoded certificate, and the certificate with the CA certificate chain. The certificate fingerprint shows the summary of the information contained in the base 64-encoded version, such as the serial number, issuing CA, validity period, and key information.

   To copy the certificate, scroll to the base 64-encoded blob and simple copy and paste.



4. To import the certificate directly into your web browser or email client, scroll to the bottom of the certificate's page, and click the **`Import ... Certificate`** button.

Importing this certificate
To import the certificate into your client, click the following button.
Import Your Certificate
Import S/MIME Certificate

2.6. Listing and Searching for Certificates

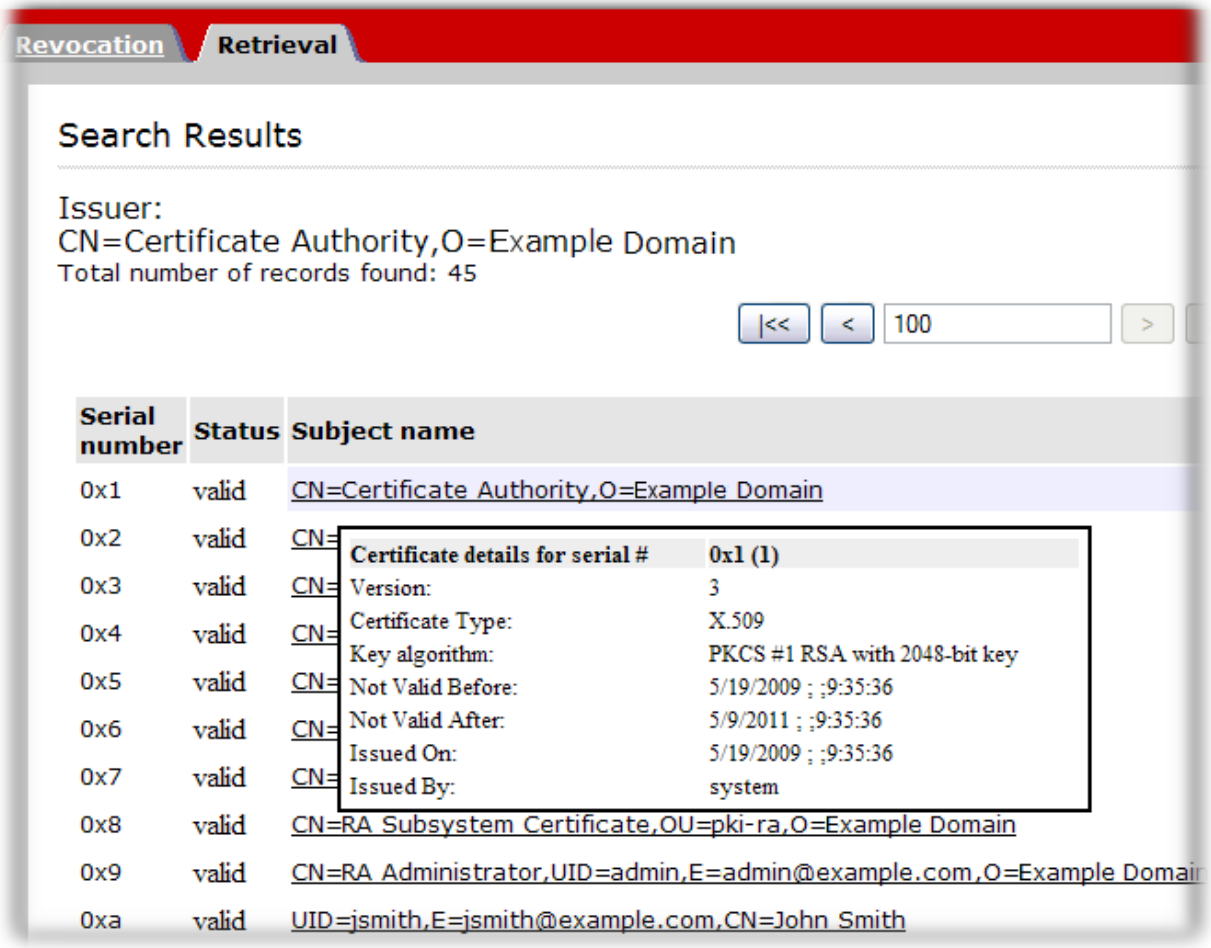
The **`Retrieval`** tab has two ways to search for certificates. The **`List Certificates`** page has a basic search for every issued certificates, while the **`Search for Certificates`** page has advanced search options which narrow down results based on specific information about the certificate.

2.6.1. Listing Certificates (Basic Search)

1. Click the **`Retrieval`** tab.
2. On the left, click the **`List Certificates`** link.
3. Fill in the serial number range and, if you want, filter out revoked or expired certificates. Leaving the lowest and highest fields blank returns all certificates that have been issued.

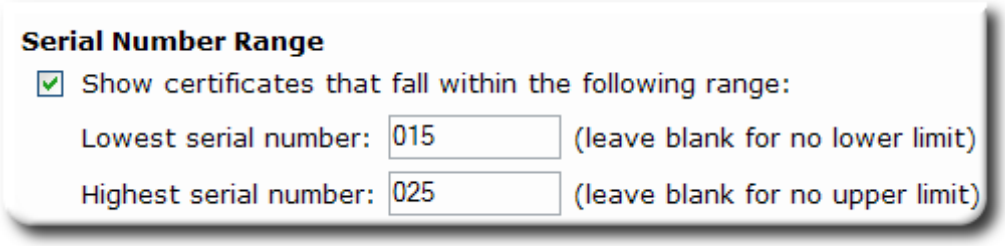
Red Hat® Certificate Manager
Enrollment
Revocation
Retrieval
Check Request Status
List Certificates
Search Certificates
Import CA Certificate Chain
Import Certificate Revocation List
List Certificates
Use this form to list certificates whose serial numbers fall within a specified range.
Enter a range of serial numbers in hexadecimal form (starting with 0x, as in the certificate list) or in decimal form.
Lowest serial number 1 (leave blank for no lower limit)
Highest serial number 55 (leave blank for no upper limit)
Do not show certificates that have been revoked
Do not show certificates that have expired or are not yet valid
Find first 100 records

4. Every certificate within that range is returned. To open the retrieval page for the certificate, click the link.

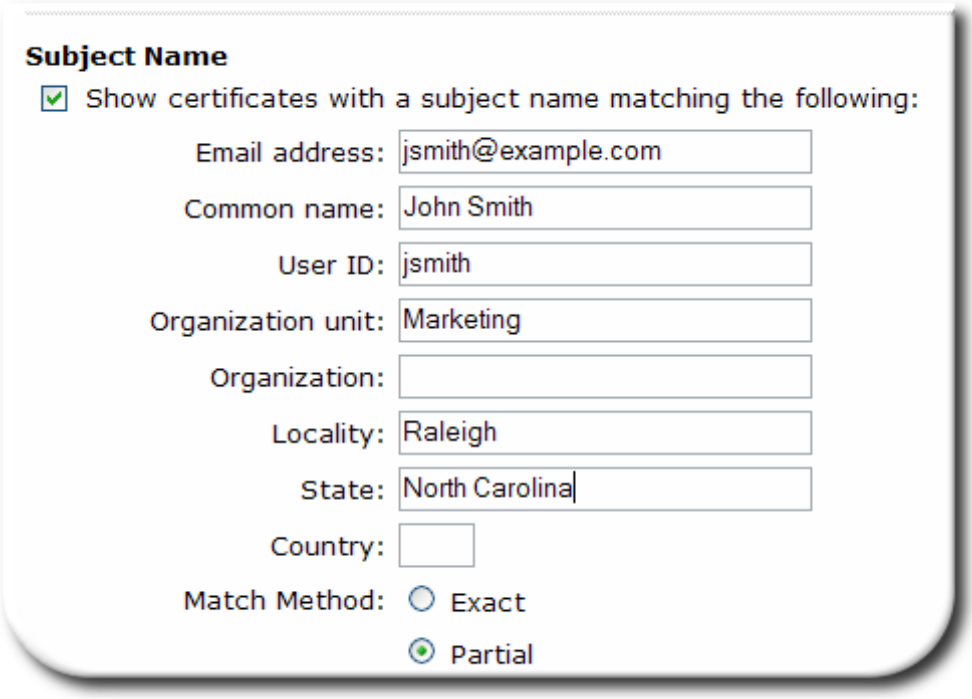


2.6.2. Searching for Certificates (Advanced Search)

1. Click the **Retrieval** tab.
2. On the left, click the **Search Certificates** link.
3. Fill in the search criteria. The **Search** form offers a number of different search areas:
   - *Serial number range* for every certificate issued within that serial number block, same as with listing certificates.


Serial Number Range
Show certificates that fall within the following range:
Lowest serial number: 015
(leave blank for no lower limit)
Highest serial number: 025
(leave blank for no upper limit)

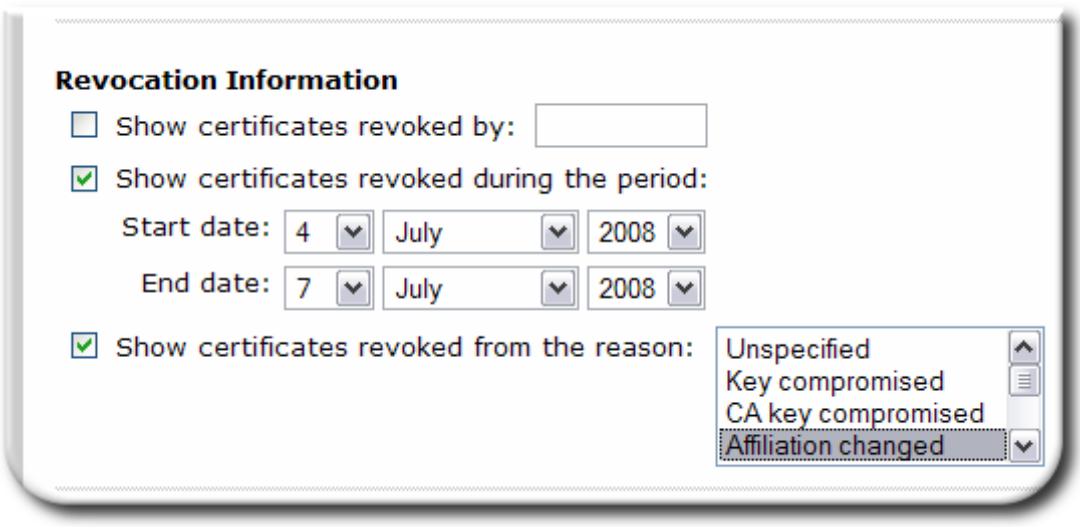
   - *Subject name*, which is a very specific search based on elements used in the subject name of the certificate, narrowing the search to the user or machine for which it was issued, or by the department, locality, or other naming element.



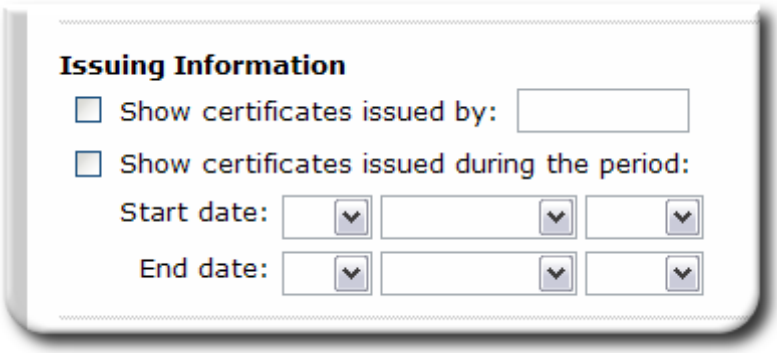
NOTE

The CA certificate request forms support all UTF-8 characters for the common name, organizational unit, and requester name fields. The common name and organization unit fields are included in the subject name of the certificate.
This support does not include supporting internationalized domain names.

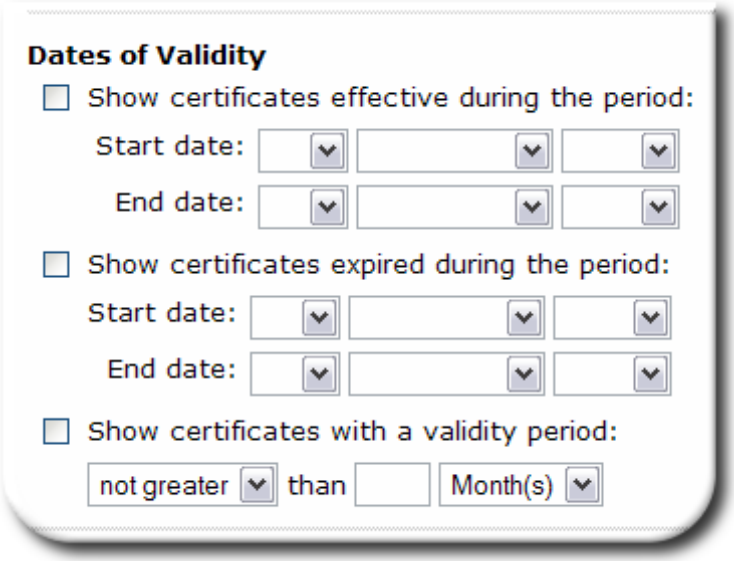
   - *Revocation status* for certificates which have been revoked. This can specify the agent or user which revoked the certificate, the date range in which the certificates were revoked, and the reason given when the certificate was revoked.



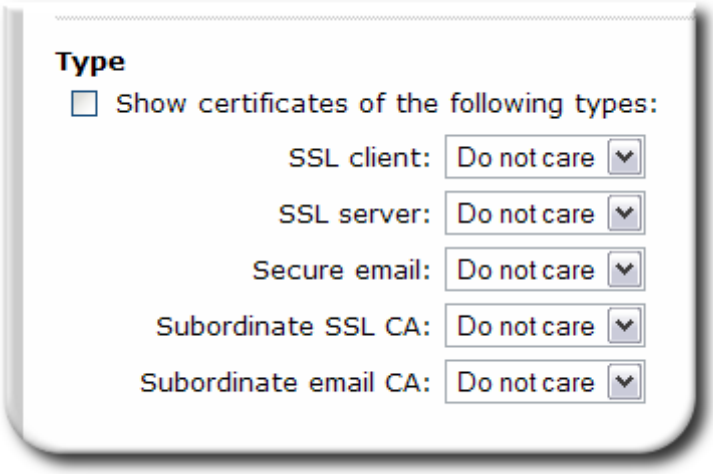
- *Issuer information*, basing the search on which Certificate Manager issued the certificate or on the dates when it was issued.



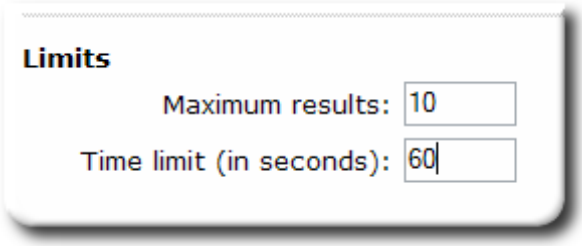
- *Validity dates*, including the range of dates when the certificate was valid (e.g., every certificate which was valid on July 4, 2008), the date range of when the certificate expired (every certificate which expired between June 1 and June 15), and how long the certificate was valid (e.g., every temporary certificate which was valid for less than 30 days).



- *Certificate type*, which can include or exclude certificates based on one of the major categories of certificates, including SSL client and server certificates and email certificates.



4. Set the search limits. The search scope can be limited in the total number of certificates returned and in how long to conduct the search.



2.7. Renewing Certificates

When certificates reach the end of their validity period, there are two ways that users can respond:

- Allow the certificate to lapse and request a new certificate. While simple, the problem in some situations is if the certificate was used to encrypt information, like emails or files. The encrypted data cannot be recovered if the certificate expires.
- Renew the certificate. Renewal takes the original keys that were generated, and regenerate the certificate with an extended validity period. Since the renewed certificate is identical to the original, everything that the original certificate did (such as decrypting files) is still possible.

NOTE

Certificates can only be renewed within a certain window of time. If you try to renew a certificate too early or too long after its expiration date, then the renewal request will fail.

There are three different certificate renewal forms,

Table 4. Enrollment Forms and Corresponding Renewal Forms

If the Renewal Form Is ...	... Then The Certificate Is Approved By ...
Self-renew user SSL client certificates	The original certificate is in your browser database. Since the original has already been approved once, then having the original automatically verifies your request.
Directory-Authenticated User Dual-Use Certificate Enrollment	The certificate is approved is you can provide the correct username and password to access the LDAP directory.
Renew certificate to be manually approved by agents	Approved by an agent.

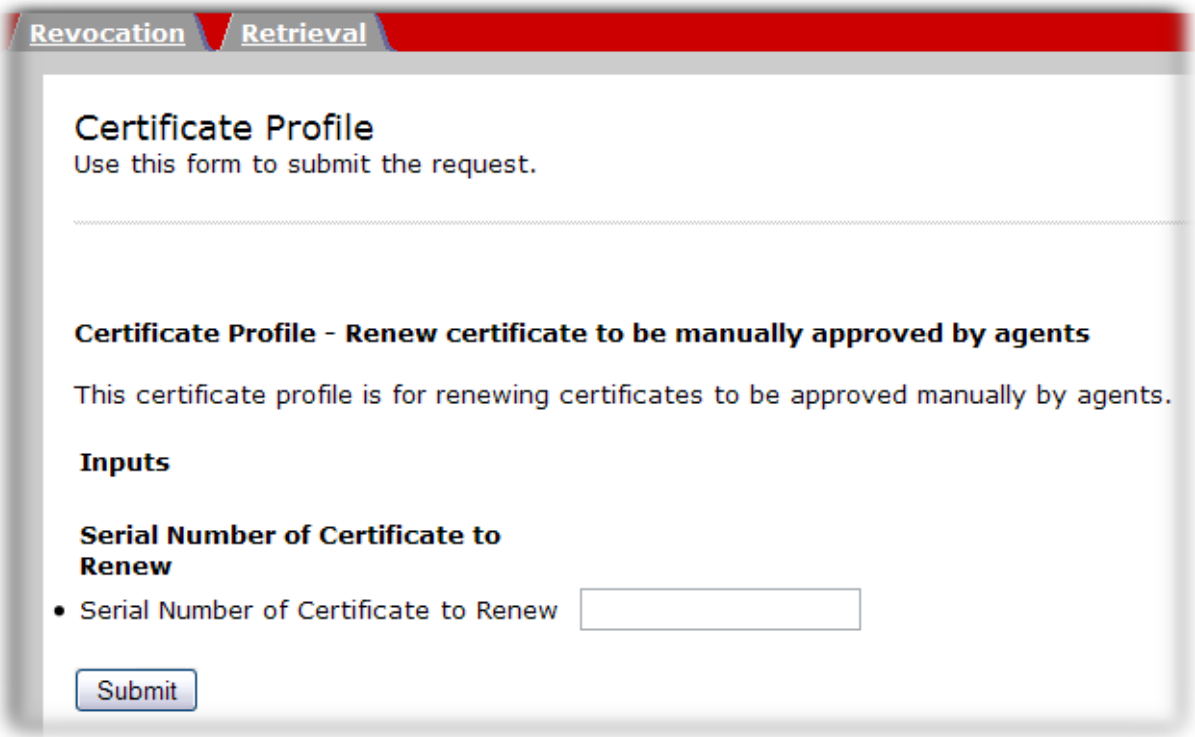
NOTE

Encryption and signing certificates (and other types of dual certificates) are created in a single step. However, the renewal process only renews one certificate at a time.
To renew both certificates in a certificate pair, each one has to be renewed individually.

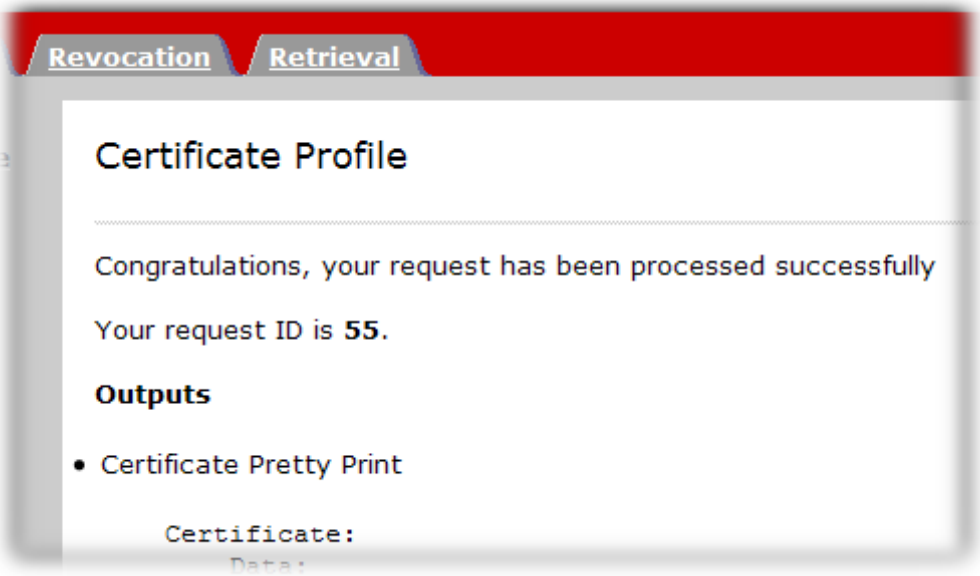
2.7.1. Agent-Approved or Directory-Based Renewals

Sometimes, a certificate renewal request has to be manually approved, either by a CA agent or by your providing login information for the user directory.

1. Click the name of the renewal form to use.
2. Enter the serial number of the certificate to renew. This can be in decimal or hexadecimal form.


Revocation
Retrieval
Certificate Profile
Use this form to submit the request.
Certificate Profile - Renew certificate to be manually approved by agents
This certificate profile is for renewing certificates to be approved manually by agents.
Inputs
Serial Number of Certificate to Renew
Serial Number of Certificate to Renew
Submit

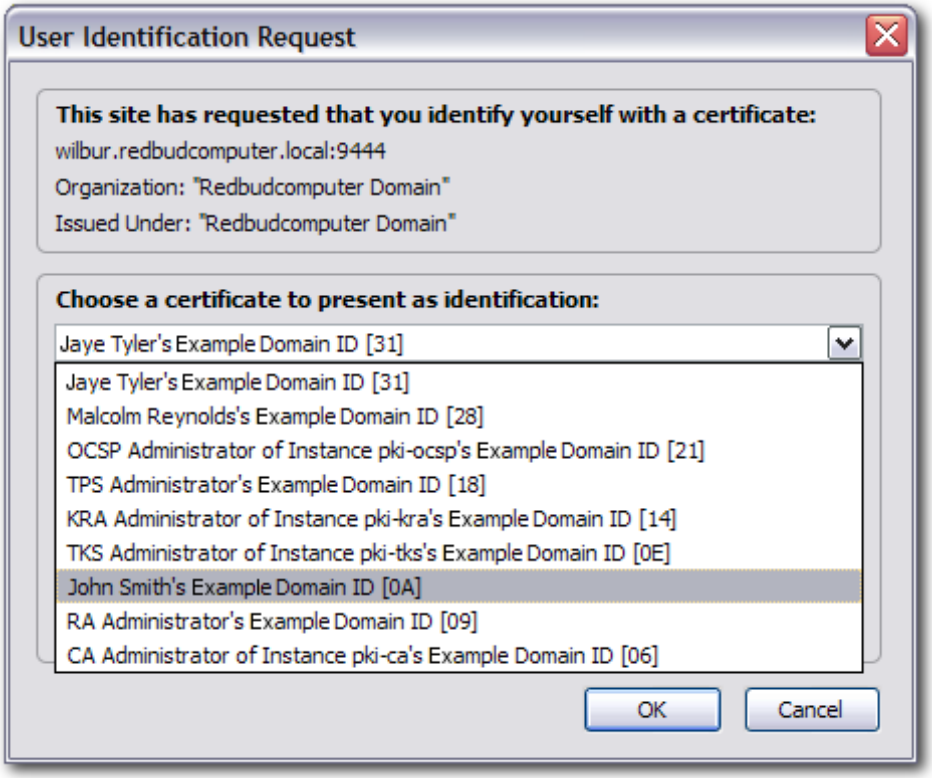
3. Click the renew button.
4. The request is submitted. For directory-based renewals, the renewed certificate is automatically returned. Otherwise, the renewal request will be approved by an agent.



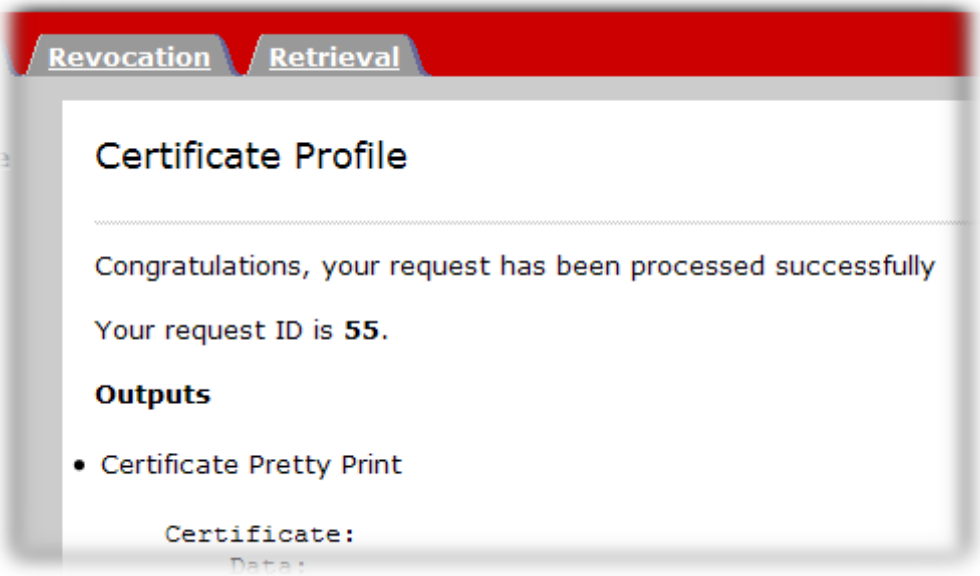
2.7.2. Certificate-Based Renewal

Some user certificates are stored directory in your browser, so some renewal forms will simply check your browser certificate database for a certificate to renew. If a certificate can be renewed, then the CA automatically approves and reissues it.

1. Click the name of the renewal form to use.
2. There is no input field, so click the **Renew** button.
3. When prompted, select the certificate to renew.


User Identification Request
This site has requested that you identify yourself with a certificate:
wilbur.redbudcomputer.local:9444
Organization: "Redbudcomputer Domain"
Issued Under: "Redbudcomputer Domain"
Choose a certificate to present as identification:
Jaye Tyler's Example Domain ID [31]
Jaye Tyler's Example Domain ID [31]
Malcolm Reynolds's Example Domain ID [28]
OCSP Administrator of Instance pki-ocsp's Example Domain ID [21]
TPS Administrator's Example Domain ID [18]
KRA Administrator of Instance pki-kra's Example Domain ID [14]
TKS Administrator of Instance pki-tks's Example Domain ID [0E]
John Smith's Example Domain ID [0A]
RA Administrator's Example Domain ID [09]
CA Administrator of Instance pki-ca's Example Domain ID [06]
OK
Cancel

4. The request is submitted and the renewed certificate is automatically returned.

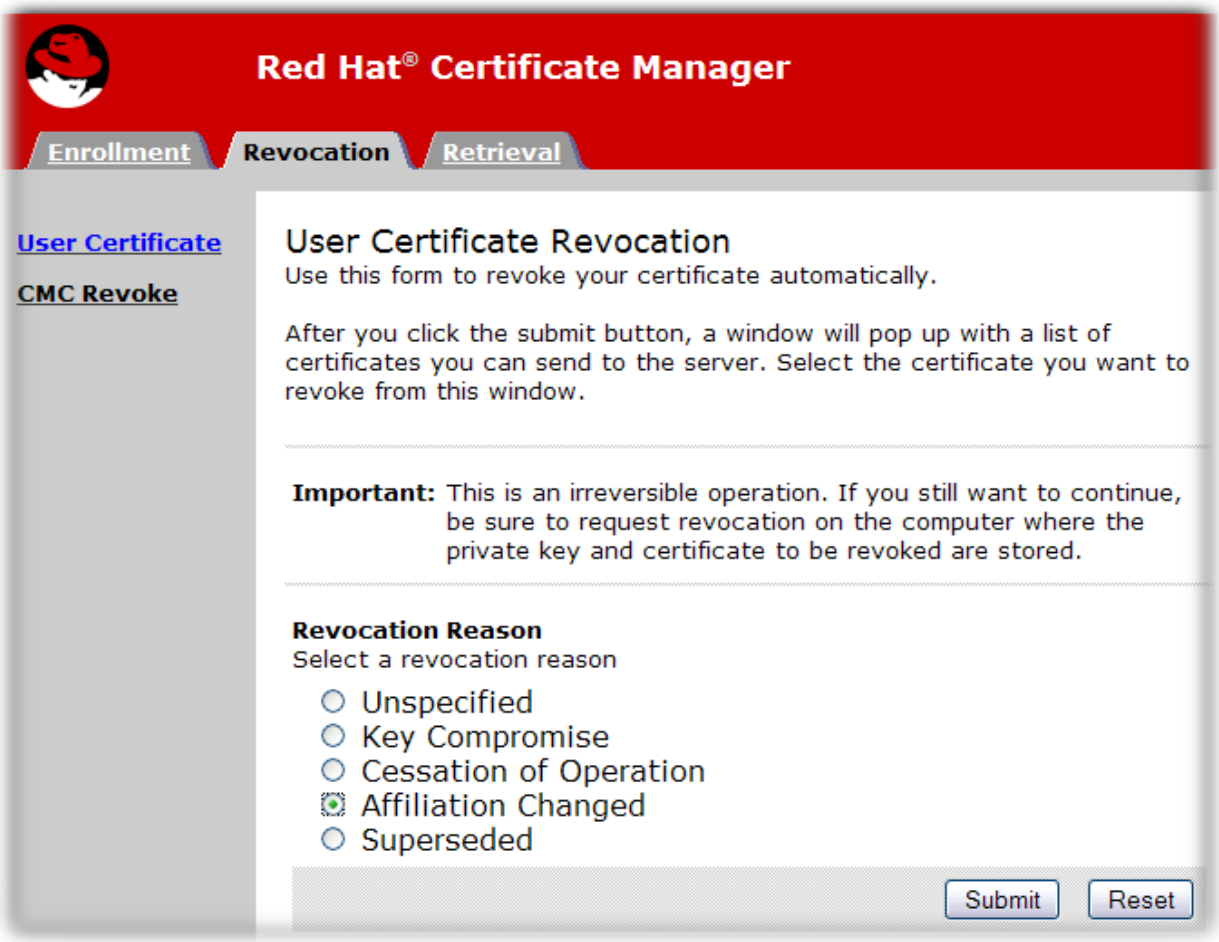


2.8. Revoking Certificates

Revoking a certificate invalidates it before its expiration date. This can be necessary if a certificate is lost, compromised, or no longer needed.

2.8.1. Revoking Your User Certificate

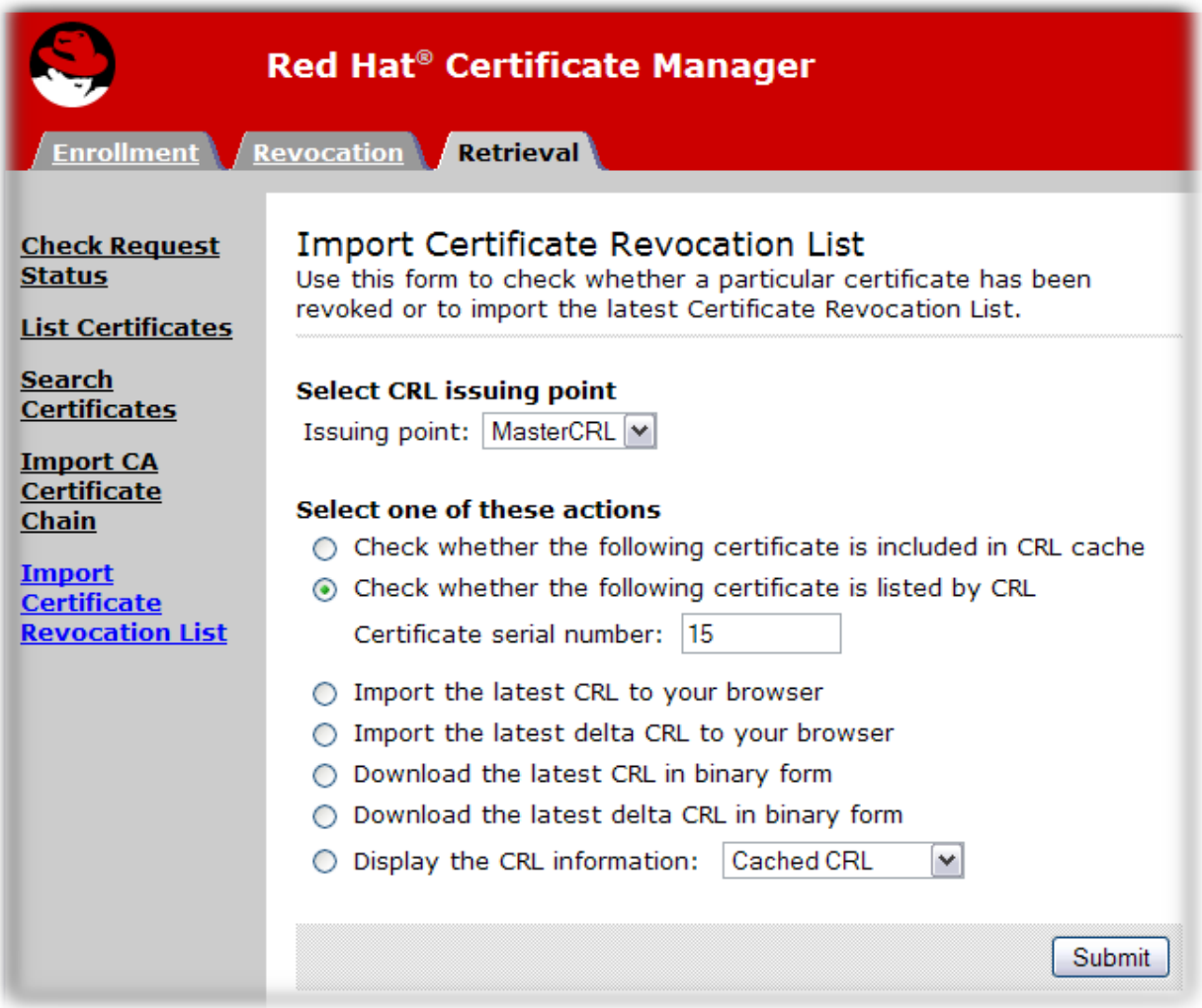
1. Click the **Revocation** tab.
2. Click the **User Certificate** link.
3. Select the reason why the certificate is being revoked, and click **Submit**.


Red Hat® Certificate Manager
Enrollment
Revocation
Retrieval
User Certificate
CMC Revoke
User Certificate Revocation
Use this form to revoke your certificate automatically.
After you click the submit button, a window will pop up with a list of certificates you can send to the server. Select the certificate you want to revoke from this window.
Important: This is an irreversible operation. If you still want to continue, be sure to request revocation on the computer where the private key and certificate to be revoked are stored.
Revocation Reason
Select a revocation reason
Unspecified
Key Compromise
Cessation of Operation
Affiliation Changed
Superseded
Submit
Reset

4. Select the certificates to revoke from the list.

2.8.2. Checking Whether a Certificate Is Revoked

1. Click the **`Retrieval`** tab.
2. Click the **`Import Certificate Revocation List`** link.
3. Select the radio button by **`Check whether the following certificate is included in CRL cache`** or **`Check whether the following certificate is listed by CRL`**, and enter the serial number of the certificate.


Red Hat® Certificate Manager
Enrollment
Revocation
Retrieval
Check Request Status
List Certificates
Search Certificates
Import CA Certificate Chain
Import Certificate Revocation List
Import Certificate Revocation List
Use this form to check whether a particular certificate has been revoked or to import the latest Certificate Revocation List.
Select CRL issuing point
Issuing point: MasterCRL
Select one of these actions
Check whether the following certificate is included in CRL cache
Check whether the following certificate is listed by CRL
Certificate serial number: 15
Import the latest CRL to your browser
Import the latest delta CRL to your browser
Download the latest CRL in binary form
Download the latest delta CRL in binary form
Display the CRL information: Cached CRL
Submit

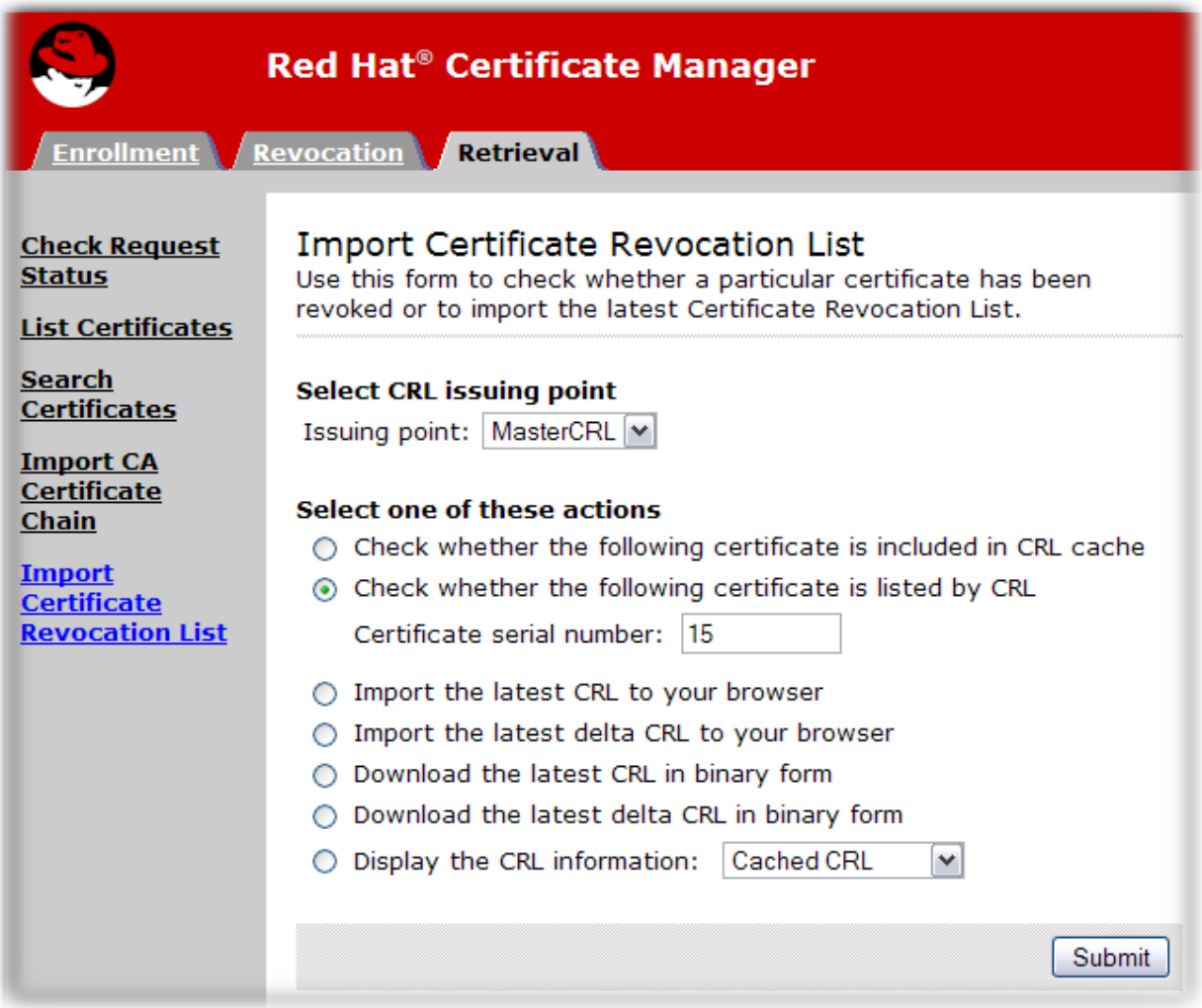
4. Click the **`Submit`** button.

   A message is returned either saying that the certificate is not listed in any CRL or giving the information for the CRL which contains the certificate.

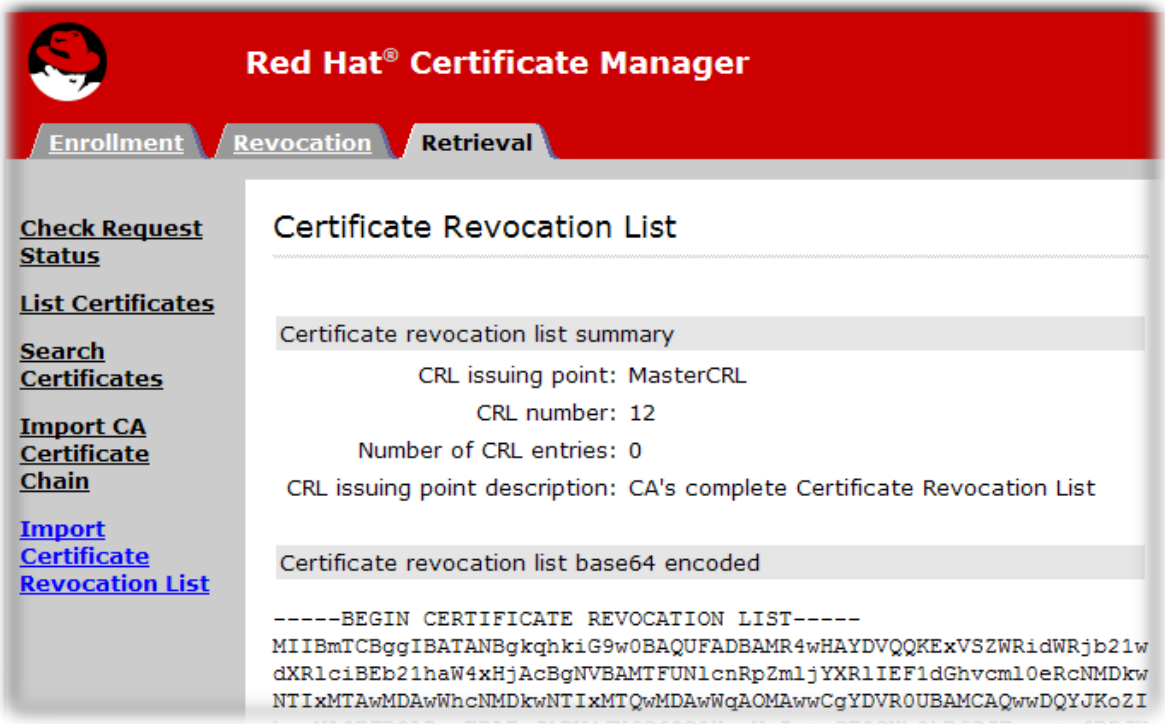
2.8.3. Downloading and Importing CRLs

Certificate revocation lists (CRLs) can be downloaded and installed in a web client, application, or machine. They can also be viewed to see what certificates have been revoked.

1. Click the **`Retrieval`** tab.
2. Click the **`Import Certificate Revocation List`** link.
3. Select the radio button to view, download, or import the CRL.


Red Hat® Certificate Manager
Enrollment
Revocation
Retrieval
Check Request Status
List Certificates
Search Certificates
Import CA Certificate Chain
Import Certificate Revocation List
Import Certificate Revocation List
Use this form to check whether a particular certificate has been revoked or to import the latest Certificate Revocation List.
Select CRL issuing point
Issuing point: MasterCRL
Select one of these actions
Check whether the following certificate is included in CRL cache
Check whether the following certificate is listed by CRL
Certificate serial number: 15
Import the latest CRL to your browser
Import the latest delta CRL to your browser
Download the latest CRL in binary form
Download the latest delta CRL in binary form
Display the CRL information: Cached CRL
Submit

- To import the CRL into the browser or download and save it, select the appropriate radio button. There are two options: to download/import the full CRL or the delta CRL. The delta CRL only imports/downloads the list of certificates which have been revoked since the last time the CRL was generated.
- To view the CRL, select **`Display the CRL information`** and select which CRL subset (called an *issuing point*) to view. This shows the CRL information, including the number of certificates included in it.

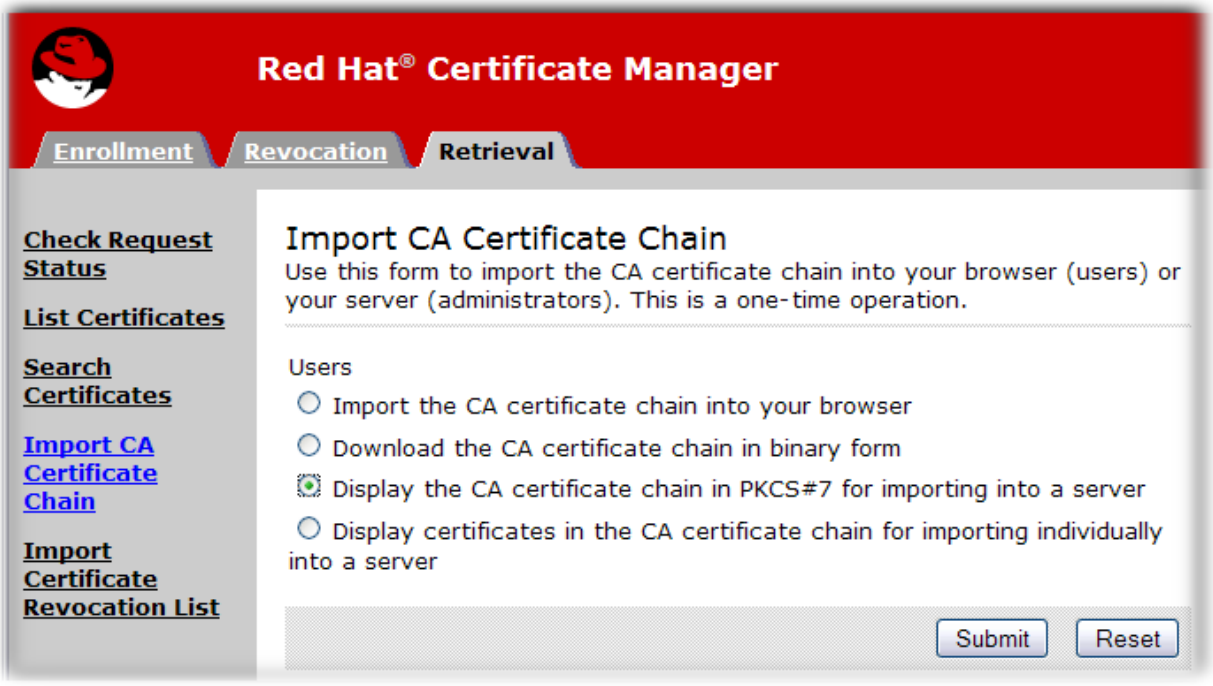


4. Click the **`Submit`** button.
5. Save the file or approve the import operation.

2.9. Downloading CA Certificates and Certificate Chains

Some services require the certificate for the Certificate Manager which issued a certificate as well as the certificate itself. The CA certificate and CA certificate chain can be downloaded, saved, and imported as needed.

1. Click the **`Retrieval`** tab.
2. Click the **`Import CA Certificate Chain`** link.
3. Select the radio button to import the CA certificate.


Red Hat® Certificate Manager
Enrollment
Revocation
Retrieval
Check Request Status
List Certificates
Search Certificates
Import CA Certificate Chain
Import Certificate Revocation List
Import CA Certificate Chain
Use this form to import the CA certificate chain into your browser (users) or your server (administrators). This is a one-time operation.
Users
Import the CA certificate chain into your browser
Download the CA certificate chain in binary form
Display the CA certificate chain in PKCS#7 for importing into a server
Display certificates in the CA certificate chain for importing individually into a server
Submit
Reset

- Import the chain into the browser.

- Save the entire CA certificate chain.
- Show the CA certificate chain in a single blob.
- Show the individual CA certificate blobs in the certificate chain.

4. Click **Submit**.
5. Save the file or complete installing the package.

3. Getting and Managing Certificates through RA Services

The Registration Authority (RA) is an intermediate subsystem between users and the Certificate Manager. This offers a way for groups to locally review and authorize certificate requests.

3.1. Opening the RA Services Page

The URL for the RA web services can vary depending on your group's server deployment. The default way to connect to the RA web services is to connect to the server over port 12890 (for SSL) or 12888. For example:

```
https://server.example.com:12890/
```

That opens a menu with links to regular user services or agent services. To get directly to the regular user pages, add **/ee/index.cgi** to the end of the URL. For example:

```
https://server.example.com:12890/ee/index.cgi
```

If DNS is properly configured, then an IPv4 or IPv6 address can be used to connect to the services pages, as well as a hostname or fully-qualified domain name. For example:

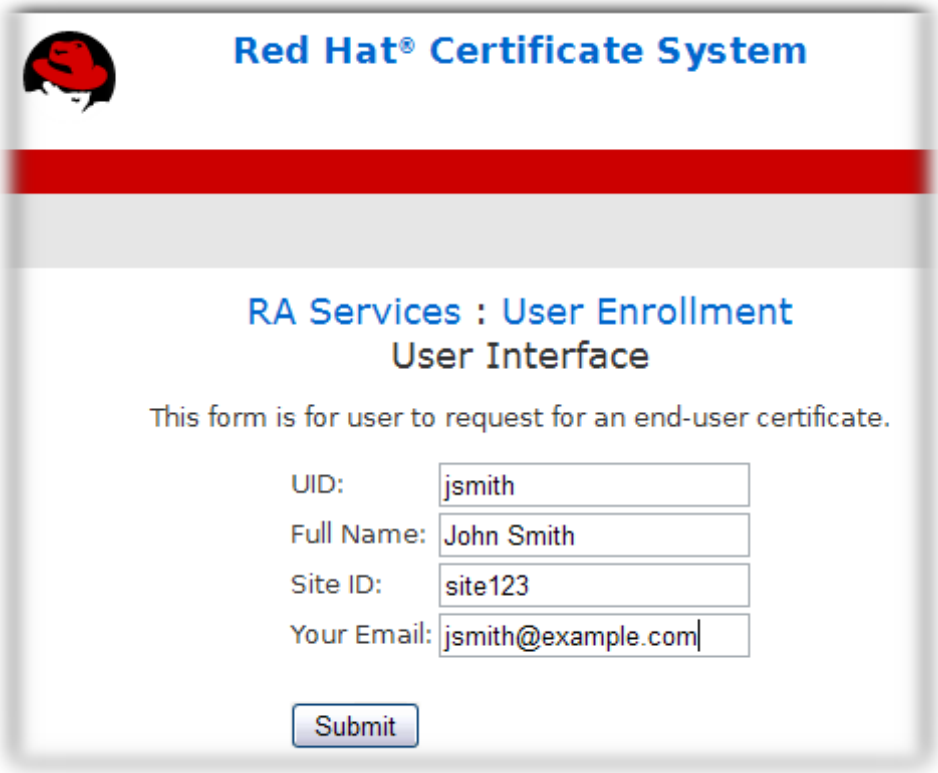
```
https://1.2.3.4:9444/ee/index.cgi
https://[00:00:00:00:123:456:789:00:]:9444/ee/index.cgi
```

3.2. Requesting Certificates

The RA user services page has submission forms for four different types of certificates.

3.2.1. Requesting User Certificates

1. In the RA services page, click the **User Enrollment** link.
2. Click the **Request Submission** link.
3. Fill in the requester information.

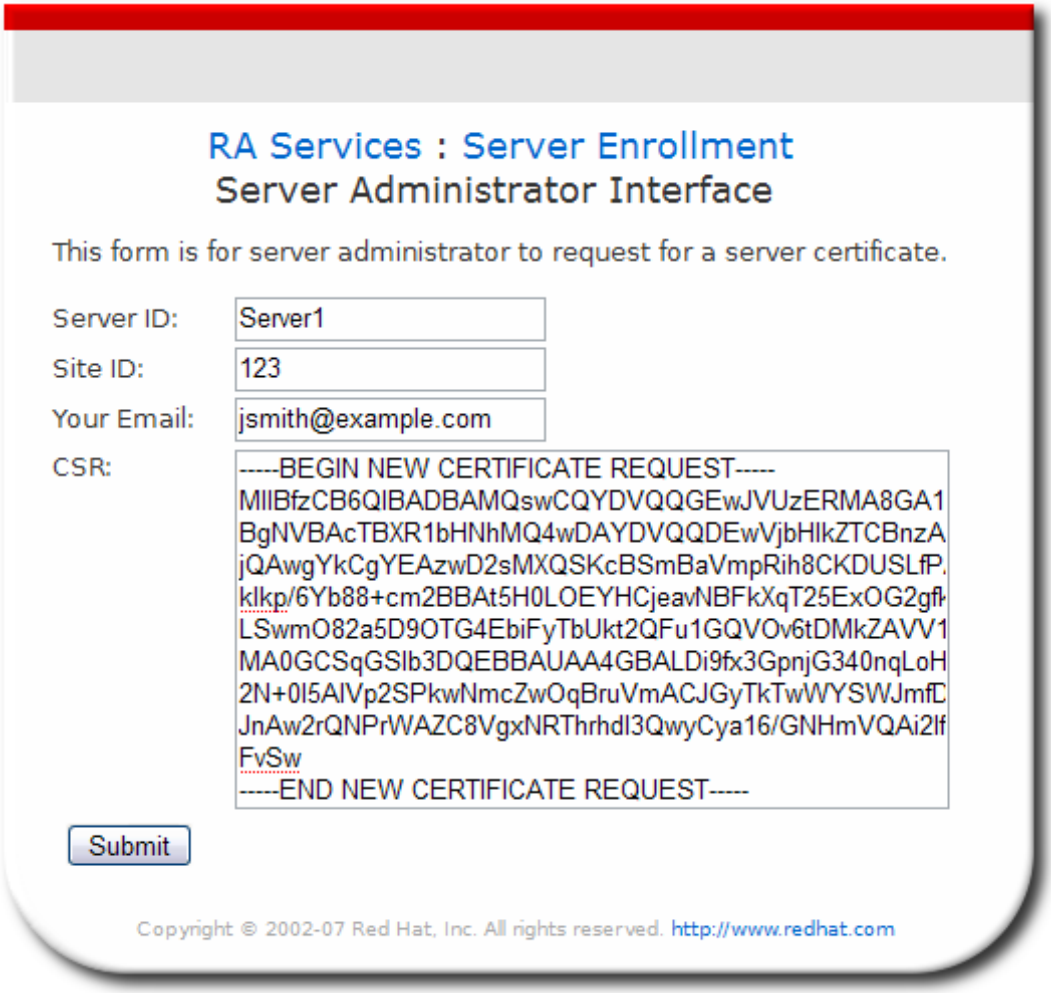


4. Click the **Submit** button.
5. Wait for the request to be generated. Check the request status and retrieve the certificate when it's issued.

3.2.2. Requesting Server Certificates

1. In the RA services page, click the **Server Enrollment** link.
2. Click the **Request Submission** link.
3. Fill in the information for the certificate request.

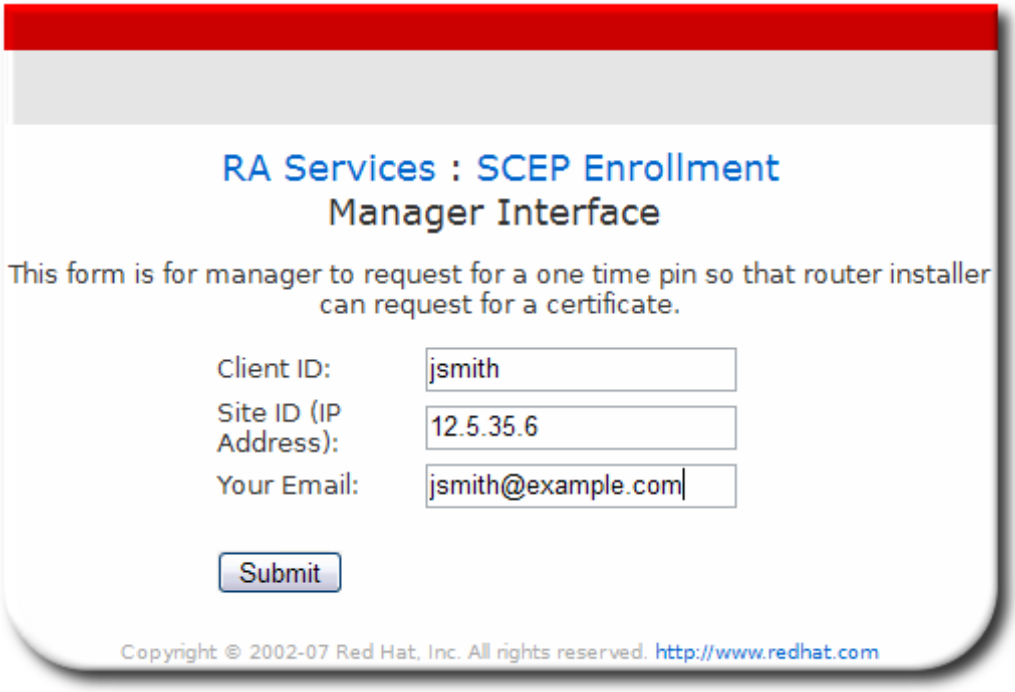
   The server certificate request requires a separately-generated certificate request. The way that you generate the base 64-encoded certificate request depends on your network setup. There may be an online form you can use to create a certificate request, the client you are requesting the certificate for may have a built-in request tool, or you can use tools such as **certutil**. The options for creating a certificate request are covered more in Section 2.2, “Generating Certificate Requests”.



4. Click the **`Submit`** button.
5. Check the request status and retrieve the certificate when it's issued.

3.2.3. Requesting SCEP (Router) Certificates

1. In the RA services page, click the **`SCEP Enrollment`** link.
2. Click the **`Pin Creation`** link.
3. Fill in the information for the certificate request.


RA Services : SCEP Enrollment
Manager Interface
This form is for manager to request for a one time pin so that router installer can request for a certificate.
Client ID:
jsmith
Site ID (IP Address):
12.5.35.6
Your Email:
jsmith@example.com
Submit
Copyright © 2002-07 Red Hat, Inc. All rights reserved. http://www.redhat.com

4. Click the **`Submit`** button.
5. Wait for the request to be generated. Check the request status and retrieve the PIN when it is issued.
6. Add the PIN and the router's ID to the **`flatfile.txt`** file so that the router can authenticate directly against the CA. For example:

```
vim /var/lib/pki-ca/conf/flatfile.txt

UID:172.16.24.238
PWD:Uojs93wkfd0IS
```

   The router's IP address can be an IPv4 address or an IPv6 address.
7. Log into the router's console. For this example, the router's name is **`scep`**:

```
scep>
```

8. Enable privileged commands.

```
scep> enable
```

9. Enter configuration mode.

```
scep# conf t
```

10. Import the CA certificate for every CA in the certificate chain, starting with the root. For example, this imports two CA certificates in the chain into the router:

```
scep(config)# crypto ca trusted-root1
scep(ca-root)# root CEP http://server.example.com:12888/ee/scep/pkiclient.cgi
scep(ca-root)# crl optional
scep(ca-root)# exit
scep(config)# cry ca authenticate 1
scep(config)# crypto ca trusted-root0
scep(ca-root)# root CEP http://server.example.com:12888/ee/scep/pkiclient.cgi
scep(ca-root)# crl optional
scep(ca-root)# exit
scep(config)# cry ca authenticate 0
```

11. Set up a CA identity, and enter the URL to access the SCEP enrollment profile. For example, for the CA:

```
scep(config)# crypto ca identity CA
scep(ca-identity)# enrollment url http://server.example.com:9180/ca/cgi-bin
scep(ca-identity)# crl optional
```

12. Get the CA's certificate.

```
scep(config)# crypto ca authenticate CA
Certificate has the following attributes:
Fingerprint: 145E3825 31998BA7 F001EA9A B4001F57
% Do you accept this certificate? [yes/no]: yes
```

13. Generate RSA key pair.

```
scep(config)# crypto key generate rsa
The name for the keys will be: scep.server.example.com
Choose the size of the key modulus in the range of 360 to 2048 for your
General Purpose Keys. Choosing a key modulus greater than 512 may take
a few minutes.

How many bits in the modulus [512]:
Generating RSA keys ...
[OK]
```

14. Lastly, generate the certificate on the router.

```
scep(config)# crypto ca enroll CA
%
% Start certificate enrollment ..
% Create a challenge password. You will need to verbally provide this
password to the CA Administrator in order to revoke your certificate.
For security reasons your password will not be saved in the configuration.
Please make a note of it.

Password: secret
Re-enter password: secret

% The subject name in the certificate will be: scep.server.example.com
% Include the router serial number in the subject name? [yes/no]: yes
% The serial number in the certificate will be: 57DE391C
% Include an IP address in the subject name? [yes/no]: yes
% Interface: Ethernet0/0
% Request certificate from CA? [yes/no]: yes
% Certificate request sent to Certificate Authority
% The certificate request fingerprint will be displayed.
% The 'show crypto ca certificate' command will also show the fingerprint.

% Fingerprint:D89DB555 E64CC2F7 123725B4 3DBDF263

Jan 12 13:41:17.348: %CRYPTO-6-CERTRET: Certificate received from
Certificate
```

15. Close configuration mode.

```
scep(config)# exit
```

16. To make sure that the router was properly enrolled, list all of the certificates stored on the router.

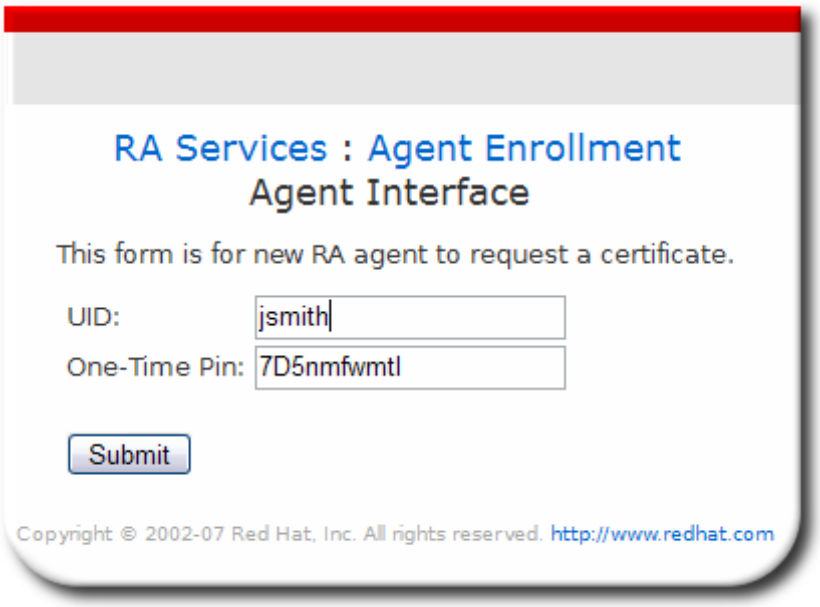
```
scep# show crypto ca certificates
Certificate
 Status: Available
 Certificate Serial Number: 0C
 Key Usage: General Purpose
 Issuer:
 CN = Certificate Authority
  O = Sfbay Red hat Domain 20070111d12
 Subject Name Contains:
 Name: scep.server.example.com
 IP Address: 10.14.1.94
 Serial Number: 57DE391C
 Validity Date:
 start date: 21:42:40 UTC Jan 12 2007
 end date: 21:49:50 UTC Dec 31 2008
 Associated Identity: CA

CA Certificate
 Status: Available
 Certificate Serial Number: 01
 Key Usage: Signature
 Issuer:
 CN = Certificate Authority
  O = Sfbay Red hat Domain 20070111d12
 Subject:
 CN = Certificate Authority
  O = Sfbay Red hat Domain 20070111d12
 Validity Date:
 start date: 21:49:50 UTC Jan 11 2007
 end date: 21:49:50 UTC Dec 31 2008
 Associated Identity: CA
```

3.2.4. Requesting Agent Certificates

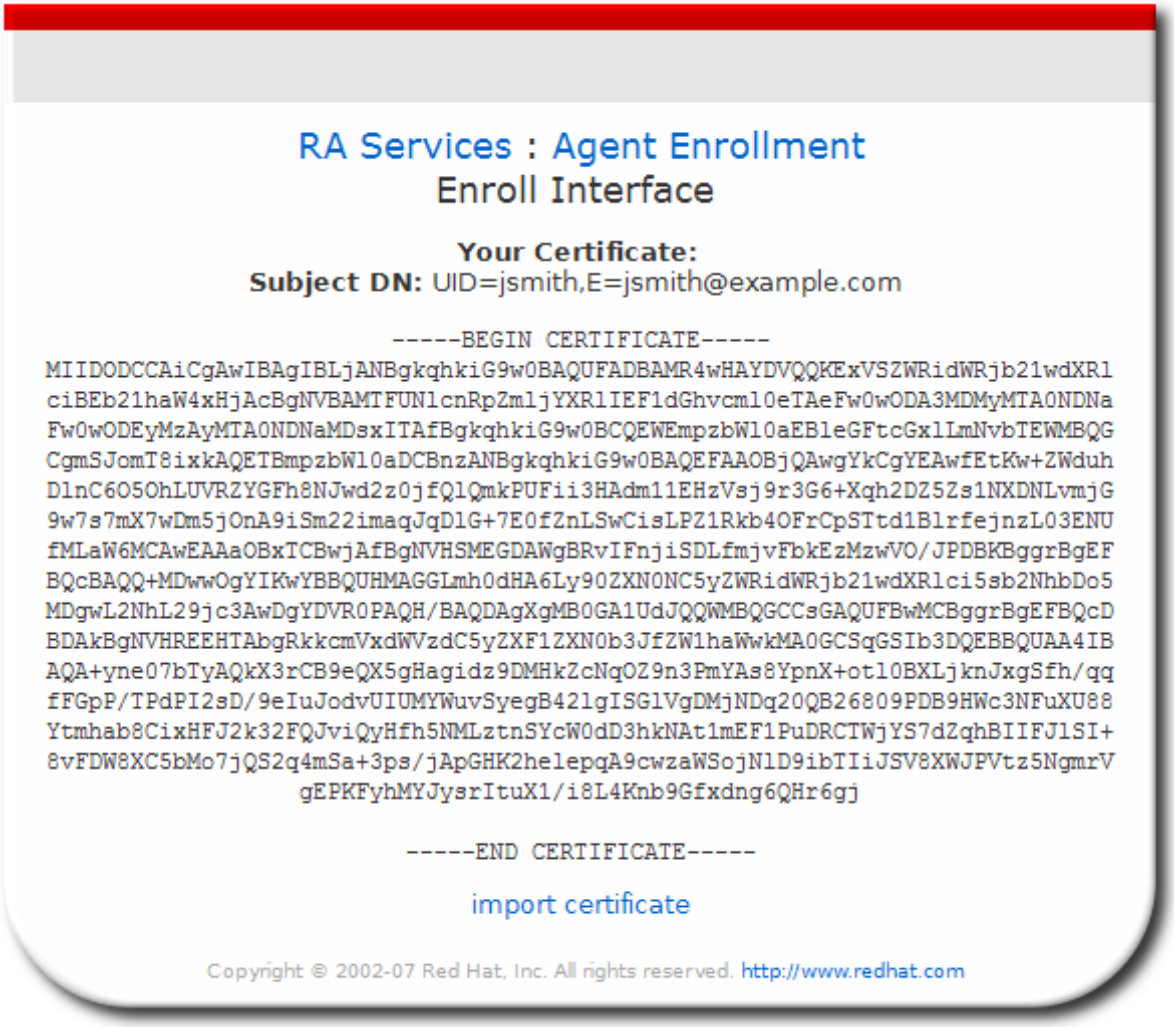
1. In the RA services page, click the **`Agent Enrollment`** link.
2. Click the **`Pin Creation`** link.
3. Fill in the information for the certificate request.

4. Click the **`Submit`** button.

5. Wait for the request to be generated. Check the request status and retrieve the PIN when it is issued.
6. Click the **Agent Enrollment** link again, and select the **Certificate Enrollment** link.
7. Enter the PIN in the enrollment form, and click **Submit**.



8. The base 64-encoded version of the certificate is displayed; this can be copied and saved to file. The agent certificate can be imported directly into the browser to enable access to the RA agent services by clicking the **Import Certificate** link at the bottom.



NOTE

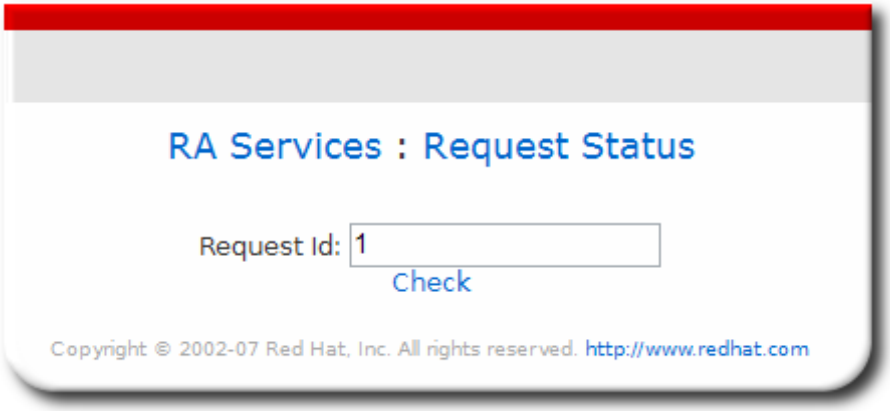
Before you can perform the operations of an RA agent, you must be added as a member to the RA agent's group. This must be done by an RA administrator; check with your Certificate System administrator to make sure that you have the required group memberships.

3.3. Checking on Your Request Status

NOTE

For user and server certificates, the certificates are retrieved through the **Status** page.

1. Click the **Request Status Check** link.
2. Enter the request ID number, and click the **Check** link. The request ID number was returned when the request was submitted.



NOTE

There is no way to search for a request ID.

3. The request status page opens. The status can be open (pending), approved, or rejected.

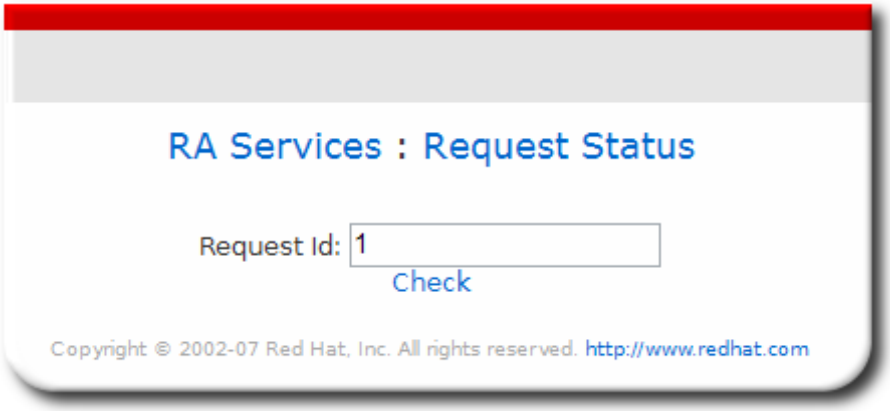
RA Services : Request Status Check
Request Status
Request ID: 1
Status: APPROVED
Error Message: 0
Import Certificate: 1
Copyright © 2002-07 Red Hat, Inc. All rights reserved. http://www.redhat.com

3.4. Retrieving and Importing Certificates

NOTE

For user and server certificates, the certificates are retrieved through the **Status** page.

1. Click the **Request Status Check** link.
2. Enter the request ID number, and click the **Check** link. The request ID number was returned when the request was submitted.



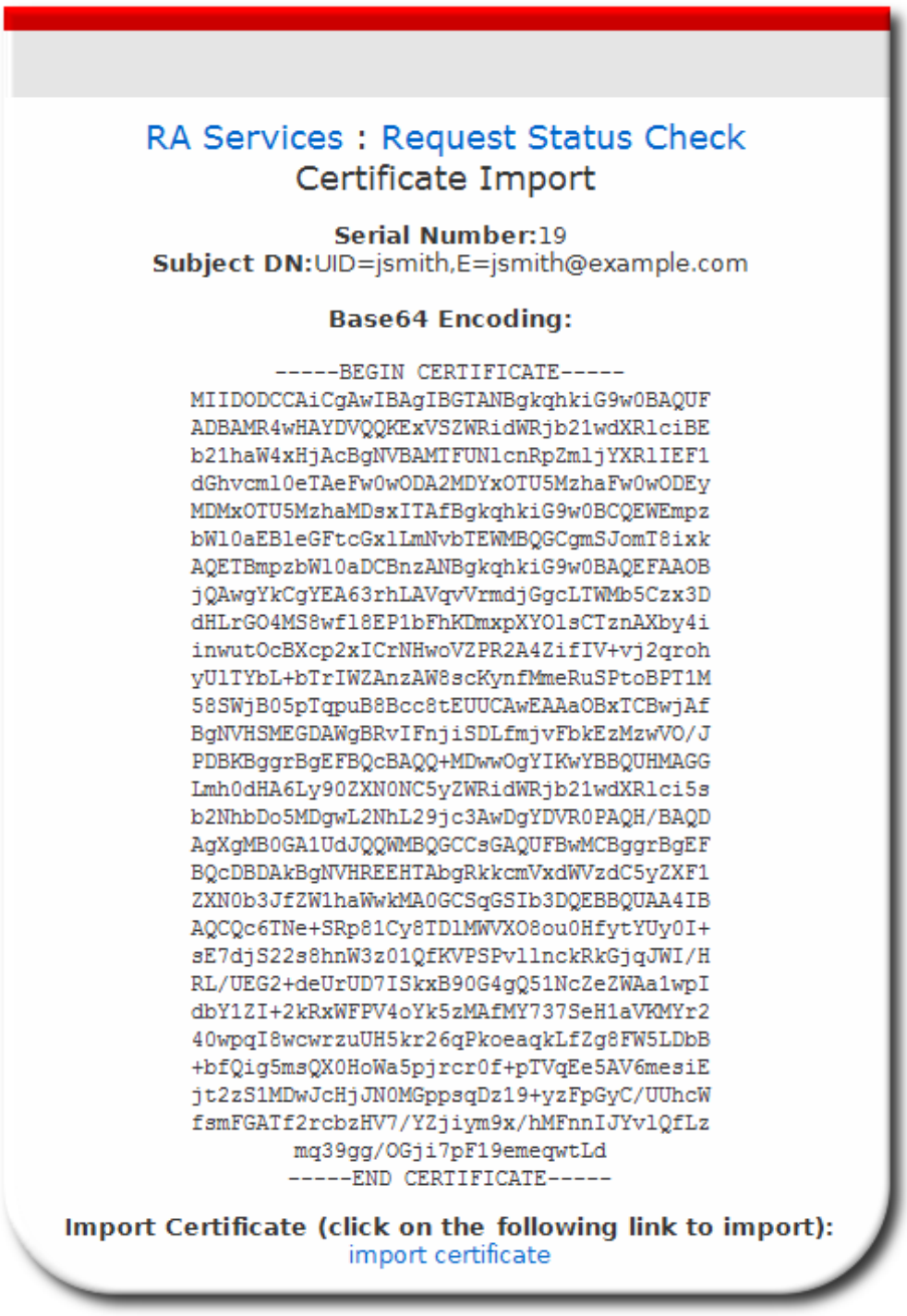
NOTE

There is no way to search for a request ID.

3. The request status page opens. If the status is **APPROVED**, then the certificate can be imported into the browser or saved to file.

RA Services : Request Status Check
Request Status
Request ID: 1
Status: APPROVED
Error Message: 0
Import Certificate: 1
Copyright © 2002-07 Red Hat, Inc. All rights reserved. http://www.redhat.com

4. If the request is approved, there will be a link by the **Import Certificate** field. Click the number, and then either copy the base 64-encoded certificate and save it to file or click the **Import Certificate** link.



3.5. Renewing User Certificates

When certificates reach the end of their validity period, there are two ways that users can respond:

- Allow the certificate to lapse and request a new certificate. While simple, a problem may occur in some situations if the certificate was used to encrypt information, like emails or files. The encrypted data cannot be recovered if the certificate expires.
- Renew the certificate. Renewal takes the original keys that were generated and regenerates the certificate with an extended validity period. Since the renewed certificate is identical to the original, everything that the original certificate did (such as decrypting files) is still possible.

NOTE

The serial number of the renewed certificate is different than that of the original certificate.

NOTE

Certificates can only be renewed within a certain window of time. If you try to renew a certificate too early or too long after its expiration date, then the renewal request will fail.

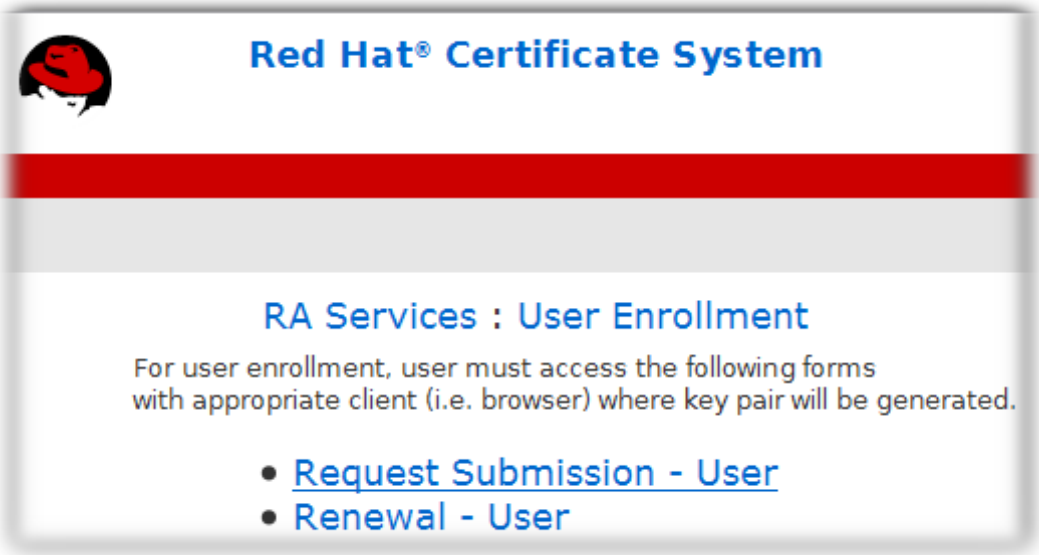
The RA allows user certificates to be renewed simply by selecting the certificate from your browsers security database.

NOTE

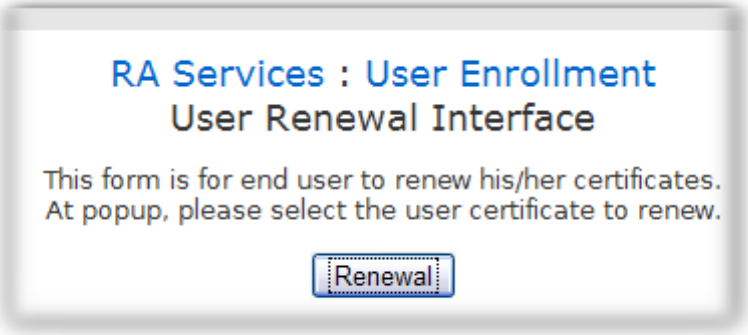
If there is no certificate imported in your browser that was processed through the RA, then the renewal attempt will fail.

To renew a certificate:

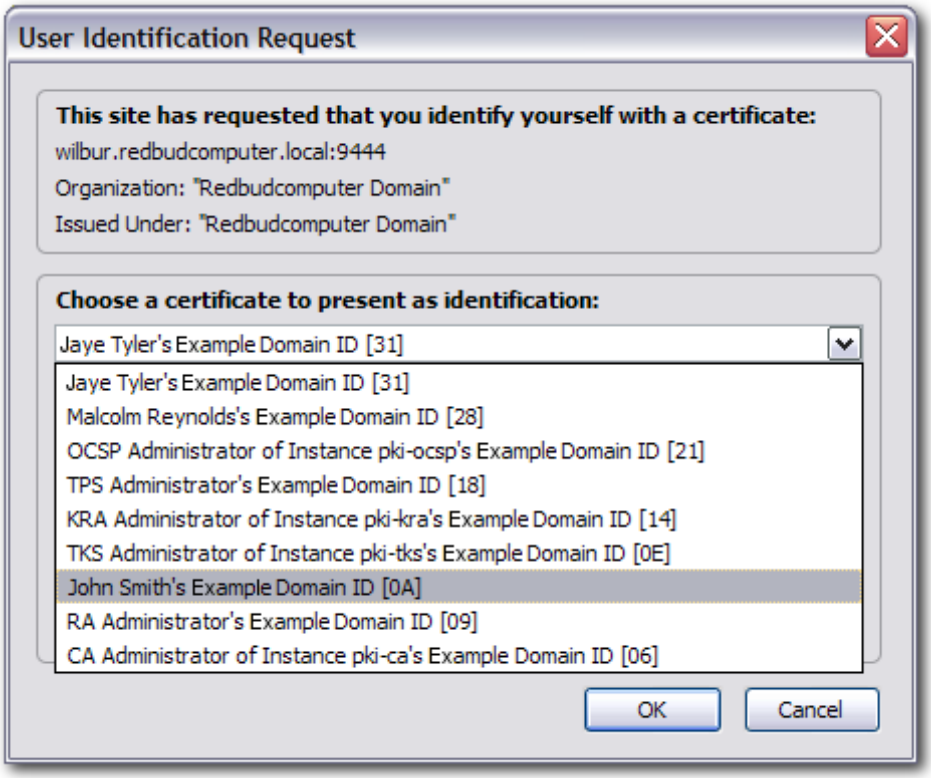
1. Click the **`User Enrollment`** link, and then the **`Renewal - User`** link.


Red Hat® Certificate System
RA Services : User Enrollment
For user enrollment, user must access the following forms
with appropriate client (i.e. browser) where key pair will be generated.
Request Submission - User
Renewal - User

2. Click the **`Renewal`** button.


RA Services : User Enrollment
User Renewal Interface
This form is for end user to renew his/her certificates.
At popup, please select the user certificate to renew.
Renewal

3. This prompts for the certificate to use from the certificates contained in your browser's security database.


User Identification Request
This site has requested that you identify yourself with a certificate:
wilbur.redbudcomputer.local:9444
Organization: "Redbudcomputer Domain"
Issued Under: "Redbudcomputer Domain"
Choose a certificate to present as identification:
Jaye Tyler's Example Domain ID [31]
Jaye Tyler's Example Domain ID [31]
Malcolm Reynolds's Example Domain ID [28]
OCSP Administrator of Instance pki-ocsp's Example Domain ID [21]
TPS Administrator's Example Domain ID [18]
KRA Administrator of Instance pki-kra's Example Domain ID [14]
TKS Administrator of Instance pki-tks's Example Domain ID [0E]
John Smith's Example Domain ID [0A]
RA Administrator's Example Domain ID [09]
CA Administrator of Instance pki-ca's Example Domain ID [06]
OK
Cancel

4. The request is submitted; it can be retrieved by using the new request ID returned, as described in Section 3.4, “Retrieving and Importing Certificates”.

4. Additional Reading

This paper covers very basic information for using the end user web services for the Certificate System CA and RA systems. That is really everything a basic end user needs to use Certificate System effectively. There are other Red Hat Certificate System resources available for the curious and for those who need to perform more advanced Certificate System functions.

For information on managing smart cards in Certificate System, see *Managing Smart Cards with the Enterprise Security Client*. This guide goes over the total functionality for the Enterprise Security Client, which handles smart cards. The *Managing Smart Cards with the Enterprise Security Client* and this *End User's Guide*, together, are both for end users of Red Hat Certificate System.

For more information on the basic concepts of certificates, public key infrastructure, and Certificate System itself, see the *Certificate System Deployment Guide*.

More detailed information about the concepts behind public key cryptography, as well as a more detailed overview of the Certificate System subsystems and how Certificate System manages certificates and smart cards, is available in the *Certificate System Administrator's Guide*. This is also the guide for administrators to manage the Certificate System server. Installation is covered in the *Certificate System Installation Guide*.

The *Certificate System Agent's Guide* covers how agents can approve and reject certificate requests and manage user certificates through other Certificate System subsystems, such as the Online Certificate Status Responder (which checks the revocation status) and the Data Recovery Manager (which recovers the certificate information if a token or a certificate is lost).

The latest information about Red Hat Certificate System, including current release notes and other

updates, is always available at the Certificate System documentation page, http://www.redhat.com/docs/manuals/cert-system/.

5. Giving Feedback

If there is any error in this *Using End User Services* or there is any way to improve the documentation, please let us know. Bugs can be filed against the documentation for Red Hat Certificate System through Bugzilla, http://bugzilla.redhat.com/bugzilla. Make the bug report as specific as possible, so we can be more effective in correcting any issues:

- Select the Red Hat Certificate System product.
- Set the component to **`Doc - end-entity-guide`**.
- Set the version number to 8.1.
- For errors, give the page number (for the PDF) or URL (for the HTML), and give a succinct description of the problem, such as incorrect procedure or typo.

  For enhancements, put in what information needs to be added and why.
- Give a clear title for the bug. For example, **`"Incorrect command example for setup script options"`** is better than **`"Bad example"`**.

We appreciate receiving any feedback — requests for new sections, corrections, improvements, enhancements, even new ways of delivering the documentation or new styles of docs. You are welcome to contact Red Hat Content Services directly at docs@redhat.com.

6. Document History

Revision 8.1-5.400	**2013-10-31**	**Rüdiger Landmann**
Rebuild with publican 4.0.0		
Revision 8.1-5	**January 31, 2012**	**Ella Deon Lackey**
Initial draft for Certificate System 8.1 documentation.		

[1] A certificate request already includes the subject name, so this information isn't required.